McDATA®

Mobilizing the World's Data™

McDATA PRODUCTS

McDATA®
Sphereon™ 4400 Fabric Switch
Installation and Service Manual

P/N 53-1000925-01

Simplifying Storage Network Management

McDATA Corporation
11802 Ridge Parkway, Broomfield, CO 80021
Corporate Headquarters: 800-545-5773
Sales E-mail: sales@mcdata.com *Web:* www.mcdata.com

Record of Revisions and Updates

Revision	Date	Description
620-000238-000	7/2005	General availability (GA) release of the manual. Describes Release 8.7 of the Enterprise Fabric Connectivity Manager application.
620-000238-010	3/2006	Upodated for ROHs changes.
620-000238-020	8/2006	Describes Release 9.0 of the Enterprise Fabric Connectivity Manager application.
53-1000925-01	3/2008	Added Japanese power cord statement.

Copyright © 2005, 2006 McDATA Corporation. All rights reserved.

Printed March 2008

Fourth Edition

With the exception of downloading a copy of this publication for the customer's own use, no part of this publication may be reproduced or distributed except as authorized under the terms of the "McDATA Corporation License to Copy Machine Readable Documentation."

The information contained in this document is subject to change without notice. McDATA Corporation assumes no responsibility for any errors that may appear.

All computer software programs, including but not limited to microcode, described in this document are furnished under a license, and may be used or copied only in accordance with the terms of such license. McDATA either owns or has the right to license the computer software programs described in this document. In addition, McDATA Corporation retains all rights, title and interest in the computer software programs.

Figures

1-1 Sphereon 4400 Fabric Switch (Front View) 1-3
1-2 Sphereon 4400 Fabric Switch (Rear View) 1-3
1-3 Management Server 1-10
1-4 24-Port Ethernet Hub 1-12
1-5 Door Key 1-14
1-6 Loopback Plug 1-14
1-7 Fiber-Optic Protective Plug 1-15
1-8 Null Modem Cable 1-15

2-1 Patch Cable and MDI Selector Configuration 2-7
2-2 Mounting Bracket Installation (Ethernet Hub) 2-8
2-3 Hardware View 2-13
2-4 Identification View 2-14
2-5 Date Time View 2-15
2-6 Parameters View 2-16
2-7 Fabric Parameters View 2-18
2-8 Network View 2-20
2-9 Basic Information View 2-21
2-10 SNMP View 2-23
2-11 SSH Configuration 2-24
2-12 OSMS View 2-25
2-13 SSL View 2-26
2-14 Maintenance Feature Installation View 2-28
2-15 Connection Description Dialog Box 2-33
2-16 1U Management Server Connections 2-36
2-17 Identification Changes Dialog Box 2-42
2-18 Internet Protocol (TCP/IP) Properties Dialog Box 2-43
2-19 Add New User Wizard 2-45
2-20 Properties Dialog Box (General Tab) 2-46

2-21 Date/Time Properties Dialog Box (Time Zone Tab) 2-47
2-22 Date/Time Properties Dialog Box (Date & Time Tab) 2-48
2-23 Add User Dialog Box 2-50
2-24 Address Properties Dialog Box (IP Address Page) 2-51
2-25 Hardware View 2-54
2-26 New Feature Key Dialog Box 2-56
2-27 Configure Date and Time Dialog Box 2-58
2-28 Identification View 2-60
2-29 Configure Switch Parameters Dialog Box 2-61
2-30 Configure Fabric Parameters Dialog Box 2-63
2-31 Configure Ports Dialog Box 2-65
2-32 Configure SNMP Dialog Box 2-67
2-33 New Threshold Alert Dialog Box 2-68
2-34 Email Event Notification Setup Dialog Box 2-71
2-35 InCD Icon (Unformatted CD) 2-75
2-36 McDATA Filecenter Home Page 2-81

3-1 Daisy-Chained Ethernet Hubs 3-18

4-1 Clean Fiber-Optic Components 4-6
4-2 McDATA Filecenter Home Page 4-7
4-3 Port List View 4-14
4-4 Diagnostics View 4-18
4-5 System Files View 4-21
4-6 Switch View 4-22
4-7 Basic Information View 4-23
4-8 Firmware Upgrade View 4-24
4-9 Backup Configuration View 4-26
4-10 Restore Configuration View 4-27
4-11 Port List View 4-35
4-12 Port Properties Dialog Box 4-39
4-13 Port Technology Dialog Box 4-40
4-14 Port Diagnostics Dialog Box 4-42
4-15 Swap Ports Dialog Box 4-44
4-16 Save Data Collection Dialog Box 4-45
4-17 Set Online State Dialog Box 4-47
4-18 Firmware Library Dialog Box 4-48
4-19 Backup and Restore Configuration Dialog Box 4-51
4-20 Reset Configuration Dialog Box 4-53
4-21 Discover Setup Dialog Box 4-54
4-22 Address Properties Dialog Box 4-54
4-23 InstallShield Wizard Dialog Box 4-56

5-1 SFP Optical Transceiver Removal and Replacement 5-4
5-2 Redundant Power Supply Removal and Replacement 5-8

6-1 Front-Accessible FRUs 6-2
6-2 Rear-Accessible FRUs 6-3
6-3 Miscellaneous Parts 6-4
6-4 Power Cords and Receptacles 6-5

B-1 InstallShield Wizard Dialog Box B-4

Tables

2-1 Factory-Set Defaults (Product) 2-1
2-2 Factory-Set Defaults (Management Server) 2-2
2-3 Installation Task Summary 2-2
2-4 Operational States and Symbols 2-53

3-1 Factory-Set Defaults 3-1
3-2 MAP Summary 3-2
3-3 Event Codes versus Maintenance Action 3-2
3-4 MAP 100 Event Codes 3-11
3-5 MAP 200 Event Codes 3-13
3-6 MAP 200 Byte 0 FRU Codes 3-13
3-7 MAP 300 Error Messages 3-17
3-8 MAP 400 Event Codes 3-25
3-9 MAP 500 Event Codes 3-27
3-10 Link Incident Messages 3-27
3-11 Invalid Attachment Reasons and Actions 3-29
3-12 Inactive Port Reasons and Actions 3-34
3-13 MAP 600 Event Codes 3-39
3-14 E_Port Segmentation Reasons and Actions 3-41
3-15 Port Fence Codes and Actions 3-46
3-16 Fabric Merge Failure Reasons and Actions 3-50

4-1 Port Operational States 4-8
4-2 Port List Table 4-14
4-3 Inspect Port Properties Table 4-15
4-4 POM Data Table 4-16
4-5 Inspect Port Transceiver Technology Table 4-16
4-6 Performance View Table 4-17

4-7 Statistical Information in Performance View 4-36
4-8 Port Properties Table 4-37
4-9 Port Technology Table 4-40

5-1 Concurrent FRUs 5-2

6-1 Front-Accessible FRU Parts List 6-2
6-2 Rear-Accessible FRU Parts List 6-3
6-3 Miscellaneous Parts List 6-4
6-4 Power Cord and Receptacle List 6-6

Contents

Preface.....xv

Chapter 1 General Information

Switch Description.....1-1
- Field-Replaceable Units.....1-2
- SFP Transceiver.....1-3
- Power Supply Assembly.....1-4

Controls, Connectors, and Indicators.....1-5
- RESET Button.....1-5
- Ethernet LAN Connector.....1-5
- Power and System Error LEDs.....1-6
- FRU Status LEDs.....1-6
- Maintenance Port.....1-6
- Chassis Ground Connector.....1-6

Switch Specifications.....1-6
Maintenance Approach.....1-8
Switch Management.....1-9
- Management Server.....1-9
- Management Server Specifications.....1-10
- Ethernet Hub (Optional).....1-11

Error-Detection, Reporting, and Serviceability Features.....1-12
Tools and Test Equipment.....1-14
- Tools Supplied with the Product.....1-14
- Tools Supplied by Service Personnel.....1-15

Chapter 2 Installation Tasks

Factory Defaults.....2-1
Installation Task Summary.....2-2

Task 1: Verify Installation Requirements 2-4
Task 2: Unpack, Inspect, and Install the Ethernet Hub (Optional) 2-5
Unpack and Inspect Ethernet Hub 2-5
Desktop Installation 2-6
Rack-Mount Installation 2-7
Task 3: Unpack, Inspect, and Install the Product 2-9
Unpack and Inspect Switch 2-9
Desktop Installation 2-9
Rack-Mount Installation 2-11
Task 4: Configure Product at the EFCM Basic Edition Interface (Optional) 2-12
Configure Product Identification 2-14
Configure Date and Time 2-15
Configure Parameters 2-16
Configure Fabric Parameters 2-17
Configure Network Information 2-19
Configure Basic Port Information 2-21
Configure Port BB_Credit 2-22
Configure Port NPIV 2-22
Configure SNMP 2-23
Enable CLI 2-24
Enable or Disable the CLI for SSH 2-24
Enable or Disable Host Control 2-25
Configure SSL Encryption 2-25
Installing PFE Keys (Optional) 2-27
Configure Security 2-29
Configure Interswitch Links 2-30
Task 5: Configure Product Network Information (Optional) .. 2-32
Task 6: Unpack, Inspect, and Install the Management Server . 2-35
Task 7: Configure Server Password and Network Addresses . 2-38
Configure Password 2-38
Configure Private LAN Addresses 2-39
Configure Public LAN Addresses (Optional) 2-39
Task 8: Configure Management Server Information 2-40
Access the Management Server Desktop 2-40
Configure Management Server Names 2-41
Configure Gateway and DNS Server Addresses 2-42
Task 9: Configure Windows Operating System Users 2-44
Change Default Administrator Password 2-44
Add a New User 2-44
Change User Properties 2-45
Task 10: Set Management Server Date and Time 2-46

Task 11: Configure the Call-Home Feature (Optional)..... 2-48
Task 12: Assign User Names and Passwords 2-49
Task 13: Configure the Product to the Management Application .. 2-51
Task 14: Record or Verify Server Restore Information..... 2-52
Task 15: Verify Product-to-Server Communication..... 2-53
Task 16: Configure PFE Key (Optional)..... 2-55
Task 17: Configure Management Server (Optional) 2-56
Task 18: Set Product Date and Time..... 2-57
Task 19: Configure the Element Manager Application 2-59
Configure Product Identification..... 2-59
Configure Product Parameters 2-61
Configure Fabric Parameters..... 2-62
Configure Ports 2-64
Configure SNMP..... 2-66
Configure Threshold Alerts..... 2-68
Enable EFCM Basic Edition and Telnet Access 2-70
Configure, Enable, and Test E-mail Notification 2-70
Configure and Enable Ethernet Events..... 2-72
Configure, Enable, and Test Call-Home Event Notification 2-72
Configure Security 2-73
Configure Interswitch Links..... 2-74
Task 20: Back Up Configuration Data..... 2-75
Task 21: Cable Fibre Channel Ports..... 2-77
Task 22: Configure Zoning (Optional)..... 2-78
Task 23: Connect Product to a Fabric Element (Optional)..... 2-79
Task 24: Register with the McDATA Filecenter..... 2-80

Chapter 3 Maintenance Analysis Procedures

Factory Defaults 3-1
Quick Start..... 3-2
MAP 0000: Start MAP..... 3-5
MAP 0100: Power Distribution Analysis..... 3-10
MAP 0200: POST Failure Analysis 3-13
MAP 0300: Loss of Server Communication..... 3-14
MAP 0400: FRU Failure Analysis 3-24
MAP 0500: Port Failure or Link Incident Analysis 3-26
MAP 0600: Fabric or ISL Problem Analysis 3-38

Chapter 4 Repair Information

Procedural Notes 4-2
Power On Switch 4-2
Power Off Switch 4-3
IML or Reset Switch 4-3
IML 4-4
Reset 4-4
Clean Fiber-Optic Components 4-5
Download Firmware or Software from the Filecenter 4-6
Port LED Diagnostics 4-8
Repair Procedures - EFCM Basic Edition 4-10
Obtaining Log Information 4-10
Performing Port Diagnostics 4-13
Collecting Maintenance Data 4-20
Setting Online State 4-21
Blocking or Unblocking a Port 4-22
Upgrading Firmware 4-23
Managing Configuration Data 4-25
Repair Procedures - SAN Management Application 4-28
Obtaining Fabric Log Information 4-29
Obtaining Switch Log Information 4-30
Performing Port Diagnostics 4-35
Collecting Maintenance Data 4-45
Setting Online State 4-46
Blocking or Unblocking a Port 4-47
Upgrading Firmware 4-48
Managing Configuration Data 4-51
Installing or Upgrading Software 4-55

Chapter 5 Removal and Replacement Procedures

Procedural Notes 5-1
ESD Procedures 5-2
Field-Replaceable Units 5-2
RRP 1: SFP Optical Transceiver 5-3
RRP 2: Redundant Power Supply 5-7

Chapter 6 Illustrated Parts Breakdown

RoHS Information 6-1
Front-Accessible FRUs 6-2
Rear-Accessible FRUs 6-3
Miscellaneous Parts 6-4
Power Cords and Receptacles 6-5

Power Cords (Japan, Denan) 6-8

Appendix A Event Code Tables

System Events (000 through 199) A-2
Power Supply Events (200 through 299) A-24
Fan Events (300 through 399) A-28
CTP Card Events (400 through 499) A-35
Port Events (500 through 599) A-39

Appendix B Restore Management Server

Requirements B-1
Restore Management Server Procedure B-2

Index I-1

Preface

This publication is part of a documentation suite that supports the McDATA® Sphereon 4400 Fabric Switch.

Who Should Use this Manual

Use this publication if you are a trained installation and service representative experienced with the product, storage area network (SAN) technology, and Fibre Channel technology.

The product contains no customer-serviceable parts that require internal access to the product during normal operation or prescribed maintenance conditions. In addition, refer to this manual for instructions prior to performing any maintenance action.

Organization of this Manual

This publication includes six chapters and two appendices organized as follows:

Chapter 1, *General Information* - This chapter describes the switch, including field-replaceable units (FRUs), controls, connectors, and indicators, and switch specifications. The chapter also describes the maintenance approach, error detection and reporting features, serviceability features, software diagnostic features, and tools and test equipment.

Chapter 2, *Installation Tasks* - This chapter describes tasks to install, configure, and verify operation of the switch, optional Ethernet hub, and rack-mount management server.

Chapter 3, *Maintenance Analysis Procedures* - This chapter describes maintenance analysis procedures (MAPs) to fault isolate a switch problem to an individual FRU.

Chapter 4, *Repair Information* - This chapter describes supplementary diagnostic and repair procedures for a failed switch. The chapter includes procedures to display and use log information, perform port diagnostics, manage configuration data, collect maintenance data, power-on, power-off, and reset the switch, set the switch online or offline, block ports, manage switch firmware, clean fiber optics, and install or upgrade management server software.

Chapter 5, *Removal and Replacement Procedures* - This chapter describes procedures to remove and replace switch FRUs.

Chapter 6, *Illustrated Parts Breakdown* - This chapter illustrates, describes, and shows the location of switch FRUs. In addition, switch FRUs are cross-referenced to corresponding part numbers.

Appendix A, *Event Code Tables* - This appendix provides an explanation of event codes that appear at the EFCM Basic Edition interface or Element Manager application. The event severity and a recommended course of action in response to each event are also provided.

Appendix B, *Restore Management Server* - This appendix provides the instructions to restore all required switch applications to the management server in case of a hard drive failure.

An *Index* is also provided.

Related Publications

Other publications that provide additional information about the switch include:

- *McDATA Products in a SAN Environment - Planning Manual* (620-000124).
- *McDATA Sphereon 4400 Fabric Switch Element Manager User Manual* (620-000241).
- *McDATA Product Safety Notices* (620-000247).
- *EFC Manager Software Release 8.7 User Manual* (620-000170).
- *McDATA EFCM Basic Edition User Manual* (620-000240).
- *McDATA SNMP Support Manual* (620-000131).
- *McDATA E/OS Command Line Interface User Manual* (620-000134).

- *McDATA EFCM Lite Installation Instructions* (958-000171).
- *1U Server Rack-Mount Kit Installation Instructions* (958-000310).
- *McDATA FC-512 Fabricenter Equipment Cabinet Installation and Service Manual* (620-000100).

Ordering Printed Manuals

To order a copy of this publication, submit a purchase order as described in *Ordering McDATA Documentation Instructions* at http://www.mcdata.com or contact your McDATA sales representative.

Where to Get Help

For technical support, McDATA end-user customers should call the phone number located on the service label attached to the front or rear of the hardware product.

McDATA's "Best in Class" Technical Support Center and Network Operations Center (NOC) provide single points of contact for customers seeking help. These centers will research, explore, and resolve inquiries or service requests regarding McDATA products and services. The centers are staffed 24 hours a day, 7 days a week, including holidays.

To expedite warranty entitlement, please have your product serial number available.

McDATA Corporation

11802 Ridge Parkway

Broomfield, CO 80021

For SAN Router issues, contact the Network Operations Center (NOC) at:

(800) 752-8061 or (763) 268-6600.

For all other products, contact the Technical Support Center at:

(800) 752-4572 or (720) 558-3910.

E-mail: support@mcdata.com

Forwarding Publication Comments

Please send comments to the McDATA technical support center by telephone, or e-mail. The numbers and e-mail address are listed above. Please identify the page numbers and details.

Trademarks

The following terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of McDATA Corporation in the United States or other countries or both:

Registered Trademarks	Trademarks
Fabricenter®	EON™
HotCAT®	OPENconnectors™
McDATA®	Sphereon™
Multi-Capable Storage Network Solutions®	
Networking the World's Business Data®	
OPENready®	
SANtegrity®	

All other trademarked terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of their respective owners in the United States or other countries or both.

Laser Compliance Statement

Product laser transceivers are tested and certified in the United States to conform to Title 21 of the Code of Federal Regulations (CFR), Subchapter J, Parts 1040.10 and 1040.11 for Class 1 laser products. Transceivers are tested and certified to be compliant with International Electrotechnical Commission IEC825-1 and European Norm EN60825-1 and EN60825-2 regulations for Class 1 laser products. Class 1 laser products are not considered hazardous. The transceivers are designed to prevent human access to laser radiation above a Class 1 level during normal operation or prescribed maintenance conditions.

Federal Communications Commission (FCC) Statement

Products generate, use, and can radiate radio frequency energy, and if not installed and used in accordance with instructions provided, may cause interference to radio communications. Products are tested and found to comply with the limits for Class A and Class B computing devices pursuant to Subpart B of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference in a residential environment. Any modification or change made to a product without explicit approval from McDATA, by means of a written endorsement or through published literature,

invalidates the service contract and voids the warranty agreement with McDATA.

Canadian EMC Statements

The statements below indicate product compliance with Interference Causing Equipment Standard (ICES) and Norme sur le Matériel Brouiller (NMB) electromagnetic compatibility (EMC) requirements as set forth in ICES/NMB-003, Issue 4.

- This Class A or Class B digital apparatus complies with Canadian ICES-003.
- Cet appareil numérique de la classe A et classe B est conforme à la norme NMB-003 du Canada.

United States and Canada UL Certification

The C-UL-US mark on a product indicates compliance with American National Standards Institute (ANSI) and Standards Council of Canada (SCC) safety requirements as tested, evaluated, and certified by Underwriters Laboratories Inc. (UL) and Underwriters Laboratories of Canada (ULC).

International Safety Conformity Declaration (CB Scheme)

A certification bodies (CB) test report supporting a product indicates safety compliance with the International Electrotechnical Commission (IEC) system for conformity testing and certification of electrical equipment (IECEE) CB scheme. The scheme is a multilateral agreement among participating countries and certification organizations that accepts test reports certifying the safety of electrical and electronic products.

European Union Conformity Declarations and Directives (CE Mark)

The CE mark on a product indicates compliance with the following regulatory requirements as set forth by European Norms (ENs) and relevant international standards for commercial and light industrial information technology equipment (ITE):

- **EN55022: 1998 -** ITE-generic radio frequency interference (RFI) emission standard for domestic, commercial, and light industrial environments, including electrical business equipment.
- **EN55024-1: 1998 -** ITE-generic electromagnetic immunity standard for domestic, commercial, and light industrial environments, including electrical business equipment.
- **EN60950/A11:1997 -** ITE-generic electrical and fire safety standard for domestic, commercial, and light industrial environments, including electrical business equipment.
- **EN61000-3-2:1995 -** ITE-generic harmonic current emissions standard for domestic, commercial, and light industrial environments (equipment with rated current less than or equal to 16 amperes per phase).
- **EN61000-3-3:1995 -** ITE-generic voltage fluctuation and flicker standard (low-voltage power supply systems) for domestic, commercial, and light industrial environments (equipment with rated current less than or equal to 16 amperes per phase).

In addition, the European Union (EU) Council has implemented a series of directives that define product safety standards for member countries. The following directives apply:

- Products conform with all protection requirements of EU directive **89/336/EEC** (Electromagnetic Compatibility Directive) in accordance with the laws of the member countries relating to EMC emissions and immunity.
- Products conform with all protection requirements of EU directive **73/23/EEC** (Low-Voltage Directive) in accordance with the laws of the member countries relating to electrical safety.
- Products conform with all protection requirements of EU directive **93/68/EEC** (Machinery Directive) in accordance with the laws of the member countries relating to safe electrical and mechanical operation of the equipment.

McDATA does not accept responsibility for any failure to satisfy the protection requirements of any of these directives resulting from a non-recommended or non-authorized modification to a product.

European Union EMC and Safety Declaration (N-Mark)

The N-mark on a product indicates compliance with European Union EMC and safety requirements as tested, evaluated, and certified by the Norwegian Board for Testing and Approval of Electrical Equipment (Norges Elektriske Materiellkontroll or NEMKO) laboratory or a NEMKO-authorized laboratory.

Argentina UL Certification

The UL Argentina plus S mark (UL-AR-S mark) on a product indicates compliance with Direccion Nacional de Comercio Interior (DNCI) Resolution Number 92/98, Phase III (for information technology equipment safety). The mark is certified by UL de Argentina, S.R.L., and accredited by the Argentine Accreditation Organization (OAA).

Australia and New Zealand C-Tick Mark

The Australia and New Zealand regulatory compliance mark (C-tick mark) on a product indicates compliance with regulatory requirements for EMC (for information technology equipment) as set forth by the Australian Communications Authority (ACA) and the Radio Spectrum Management Group (RSM) of New Zealand.

People's Republic of China CCC Mark

The China Compulsory Certification mark (CCC mark) on a product indicates compliance with People's Republic of China regulatory requirements for safety and EMC (for information technology equipment) as set forth by the National Regulatory Commission for Certification and Accreditation.

Chinese National Standards Statement

The Taiwanese Bureau of Standards, Metrology, and Inspection mark (BSMI mark) and the Chinese National Standards (CNS) statement below indicate product compliance with Taiwanese regulatory requirements. The statement indicates in a domestic environment the product may cause radio interference, in which case the user is required to take corrective actions.

這是乙類的資訊產品，在居住環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

German GS Mark

The Geprüfte Sicherheit mark (GS mark) on a product indicates compliance with the German Safety of Equipment Act as tested by Underwriters Laboratories International Demko A/S, and accredited by the Central Office of Safety of the German Länder (Zentralstelle der Länder für Sicherheitstechnik or ZLS).

Japanese VCCI Statement

The Voluntary Control Council for Interference (VCCI) statement below applies to information technology equipment, and indicates product compliance with Japanese regulatory requirements. The statement indicates a product is a Class A or Class B product, and in a domestic environment may cause radio interference, in which case the user is required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean MIC Mark

The Korean Ministry of Information and Communications mark (MIC mark) on a product indicates compliance with regulatory requirements for safety and EMC (for information technology equipment) as authorized and certified by the Korean Radio Research Institute (RRI).

Mexican NOM Mark

The Official Mexican Standard (Normas Oficiales Mexicanas or NOM) mark on a product indicates compliance with regulatory requirements for safety (for information technology equipment) as authorized and accredited by the National System of Accreditation of Testing Laboratories (Sistema Nacional de Acreditamieno de Laboratorios de Pruebas or SINALP).

Russian GOST Certification

The Russian Gosudarstvennyi Standart (GOST) mark on a product indicates compliance with regulatory requirements for safety and EMC (for information technology equipment) as authorized and accredited by the State Committee for Standardization, Metrology and Certification.

South African SABS Certification

The South African Bureau of Standards (SABS) mark on a product indicates compliance with regulatory requirements for safety and EMC (for information technology equipment) as authorized and accredited by the Independent Communications Authority of South Africa (ICASA).

European Union Waste Managment Information

Do not discard a product. European Union Directive 2002/96/EC requires a product to be recycled at the end of its useful life. Follow all waste management actions defined by this directive. Directive requirements may be superseded by EU member nation law. Perform the following to identify pertinent information:

1. Review the original purchase contract to determine a contact regarding waste management of a product, or
2. Contact the company from which a product was procured.

Danger and Attention Statements

The following **DANGER** statements appear in this publication and describe safety practices that must be observed while installing or servicing the product. A **DANGER** statement provides essential information or instructions for which disregard or noncompliance may result in death or severe personal injury.

DANGER statements have a numerical ID (displayed in parentheses) at the end of each statement. Use the numerical ID to locate translated statements in the *McDATA Product Safety Notices* (620-000247) manual delivered with the product.

DANGER

Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded. (D004)

DANGER

Disconnect the power cords. (D005)

The following **ATTENTION** statements appear in this publication and describe practices that must be observed while installing or servicing a product. An **ATTENTION** statement provides essential information or instructions for which disregard or noncompliance may result in equipment damage or loss of data.

ATTENTION ! Prior to servicing a product, management server, or customer-supplied server, determine the Ethernet LAN configuration. Installation of products and servers on a public customer intranet can complicate problem determination and fault isolation.

ATTENTION ! Activating a preferred path can result in receipt of out-of-order frames if the preferred path differs from the current path, if input and output (I/O) is active from the source port, and if congestions is present on the current path.

ATTENTION ! Do not remove a power supply unless a replacement FRU is immediately available. To avoid product overheating, a removed power supply must be replaced within five minutes.

ATTENTION ! A reset should only be performed if a CTP card failure is indicated. Do not reset a managed product unless directed to do so by a procedural step or the next level of support.

ATTENTION ! This procedure deletes all data from the C: hard drive partition.

ATTENTION ! Contents of the data directory are backed up to the management server's CD-RW drive when directory contents change. To ensure trouble-free backups, always leave a CD in the drive. Ensure data is not being written to or read from the CD-RW drive before removing the CD. Removing the CD during a backup or restore operation can corrupt data.

General Precautions

When installing or servicing the product, follow these practices:

- Always use correct tools.
- Always use correct replacement parts.
- Keep all paperwork up to date, complete, and accurate.

ESD Precautions

Follow these electrostatic discharge (ESD) procedures:

- If the product is connected to facility power (grounded), wear an ESD wrist strap and grounding cable connected to the product chassis.
- If the product is not connected to facility power (not grounded), wear an ESD wrist strap and grounding cable connected to an approved bench grounding point.
- Touch the product chassis once before performing a procedure, and once each minute during the procedure.
- Store ESD-sensitive FRUs in antistatic packaging.

1 General Information

The McDATA® Sphereon™ 4400 Fabric Switch provides 16 ports of low-cost and high-performance dynamic Fibre Channel connectivity for switched fabric or arbitrated loop devices. This function allows low-cost, low-bandwidth workgroup (edge) devices to communicate with mainframe servers, mass storage devices, or other peripherals, and ultimately be incorporated into an enterprise storage area network (SAN) environment. This chapter describes:

- The switch, including field-replaceable units (FRUs), controls, connectors, indicators, and specifications.
- Maintenance approach.
- Switch management.
- Error detection, reporting, and serviceability features.
- Tools and test equipment.

Switch Description

The switch provides Fibre Channel connectivity through generic mixed ports (GX_Ports). Ports operate at 1.0625, 2.1250, or 4.2500 gigabits per second (Gbps), and can be configured as:

- Fabric ports (F_Ports) to provide direct connectivity for switched fabric devices.

- Expansion ports (E_Ports) to provide interswitch link (ISL) connectivity to fabric directors and switches.
- Fabric loop ports (FL_Ports) to provide connectivity and fabric attachment for Fibre Channel arbitrated loop (FC-AL) devices.

The switch is installed on a table or desktop, mounted in an FC-512 Fabricenter® equipment cabinet, or mounted in any standard 19-inch equipment rack.

Operators with a browser-capable PC and Internet connectivity can manage the switch through a firmware-resident Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface. The interface manages only a single switch, and provides a graphical user interface (GUI) that supports configuration, statistics monitoring, operation, and maintenance. The interface is opened from a web browser running Netscape Navigator® 4.6 (or higher) or Microsoft® Internet Explorer 4.0 (or higher).

As an option, the switch is managed through a one-unit (1U) high, rack-mount management server running a Java™-based SAN management application (EFCM 8.7 or later) and the switch Element Manager application.

Multiple switches and the 1U server communicate on a local area network (LAN) through one or more 10/100 Base-T Ethernet hubs. The 24-port Ethernet hubs are optional and ordered with the switch. Up to three hubs are daisy-chained as required to provide additional Ethernet connections as more switches (or other managed products) are installed on a network.

Field-Replaceable Units

The switch provides a modular design that enables quick removal and replacement of FRUs, including small form factor pluggable (SFP) optical transceivers and power supply assemblies. Figure 1-1 illustrates the front of the switch and shows the:

1. **RESET** button.
2. Ethernet LAN connector.
3. Green power (**PWR**) light-emitting diode (LED).
4. Amber system error (**ERR**) LED.
5. SFP optical transceivers (16).
6. Chassis ground (**GND**) connector.

Figure 1-1 Sphereon 4400 Fabric Switch (Front View)

Figure 1-2 illustrates the rear of the switch and shows the:

1. RS-232 maintenance port.
2. External power supply connectors (2).

Figure 1-2 Sphereon 4400 Fabric Switch (Rear View)

SFP Transceiver

Multimode fiber-optic cables attach to switch ports through SFP transceivers with duplex LC® connectors, and can be detached from switch ports (through a 10-pin interface) for easy replacement. Tri-rate (1.0625, 2.1250, or 4.2500 Gbps) shortwave laser transceivers (850 nm) provide connectivity:

- At 500 meters (1.0625 Gbps) through 50-micron multimode fiber-optic cable.
- At 300 meters (2.1250 Gbps) through 50-micron multimode fiber-optic cable.
- At 150 meters (4.2500 Gbps) through 50-micron multimode fiber-optic cable.
- At 300 meters (1.0625 Gbps) through 62.5-micron multimode fiber-optic cable.
- At 150 meters (2.1250 Gbps) through 62.5-micron multimode fiber-optic cable.
- At 70 meters (4.2500 Gbps) through 62.5-micron multimode fiber-optic cable.

Tri-rate longwave laser (1.0625, 2.1250, or 4.2500 Gbps) are also available. Longwave laser transceivers provide connectivity at 4 kilometers and 10 kilometers through singlemode fiber-optic cable. (Additional distances will be available in the future. 2Gb LW optics are currently available for 10, 20, 35 and 80 kilometers.)

The switch also provides a predictive optics monitoring (POM) feature that monitors operation of SFP optical transceivers. Digital diagnostics-enabled optical transceivers report temperature, voltage current, transceiver power, and receiver power to product firmware. Optical transceivers also provide vendor-specific threshold values for these parameters.

Power Supply Assembly

The switch is delivered with one external power supply assembly. The power supply steps down and rectifies facility input power to provide 12 volts direct current (VDC) to the control processor (CTP) card. The power supply also provides input filtering, overvoltage protection, and overcurrent protection. The power supply is input rated at 100 to 240 volts alternating current (VAC).

A second power supply can be installed as an option. When a second power supply is detected, the switch automatically enables high availability (HA) mode. With HA mode enabled, either power supply can be replaced while the switch is operational. Each power supply has a separate connection to the CTP card to allow for independent AC power sources.

Three internal cooling fans provide airflow for the CTP card, as well as redundancy for continued operation if a single fan fails.

Controls, Connectors, and Indicators

Controls, connectors, and indicators for the switch include the:

- **RESET** button.
- Ethernet LAN connector.
- Green **PWR** and amber **ERR** LEDs.
- Green and amber status LEDs associated with FRUs.
- RS-232 maintenance port.
- Chassis ground (**GND**) connector.

RESET Button

When the **RESET** button is pressed, held for three seconds, and released, the switch performs an initial machine load (IML) that reloads the firmware from FLASH memory. This operation is not disruptive to Fibre Channel traffic. When the **RESET** button is pressed and held for ten seconds, the switch performs a reset. After three seconds, the **ERR** LED blinks at twice the unit beaconing rate. A reset is disruptive to Fibre Channel traffic and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the management server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

Perform a reset only if a CTP card failure is indicated. The button is flush mounted to protect against inadvertent activation.

Ethernet LAN Connector

The front panel has a 10/100 megabit per second (Mbps) RJ-45 twisted-pair connector that attaches to an Ethernet LAN to provide communication with a management server or simple network management protocol (SNMP) workstation.

The connector provides two green LEDs. The left LED illuminates to indicate LAN operation at 10 Mbps. The right LED illuminates to indicate operation at 100 Mbps.

Power and System Error LEDs

The **PWR** LED illuminates when the switch is connected to facility AC power and is operational (the product does not have a power switch). If the LED extinguishes, a facility power source, power cord, or power distribution failure is indicated.

The **ERR** LED illuminates when the switch detects an event requiring operator attention, such as a FRU failure. The LED illuminates as long as an event is active. The LED extinguishes when *Clear System Error Light* is selected from the EFCM Basic Edition interface or Element Manager application. The **ERR** LED also blinks if unit beaconing is enabled. An illuminated LED (indicating a failure) takes precedence over unit beaconing.

FRU Status LEDs

Amber and green LEDs associated with switch FRUs provide status information as follows:

- **Fibre Channel ports -** LEDs above or below each port illuminate, extinguish, or blink to indicate port status and speed. The amber LED illuminates if the port fails. The green LED illuminates to indicate 1.0625, 2.1250, or 4.2500 Gbps port operation.
- **Power supply assembly -** A green LED on each external assembly illuminates when the FRU is operational.

Maintenance Port

The rear panel has a 9-pin DSUB maintenance port that provides a connection for a local terminal or dial-in connection for a remote terminal. The port is typically used only by maintenance personnel, however operators can use the port to configure network addresses.

Chassis Ground Connector

The front panel has a chassis ground connector for an electrostatic discharge (ESD) wrist strap and grounding cable. Plug the grounding cable into the connector when performing a maintenance action with the switch connected to facility power (grounded).

Switch Specifications

This section lists physical characteristics, storage and shipping environment, operating environment, and service clearances.

Physical Characteristics

Dimensions:

Height: 4.1 centimeters (1.6 inches) or 1 rack unit

Width: 19.9 centimeters (7.8 inches)

Depth: 33.3 centimeters (13.1 inches), plus 6.1 centimeters (2.4 inches) for external power supplies

Weight: 4.0 kilograms (8.8 pounds)

Power requirements:

Input voltage: 100 to 240 VAC

Input current: 3.5 amps at 208 VAC

Input frequency: 50 to 60 Hz

Heat dissipation:

42 watts (143 BTUs/hr)

Cooling airflow clearances (switch chassis):

Right and left side: 1.3 centimeters (0.5 inches)

Front and rear: 7.6 centimeters (3.0 inches)

Top and bottom: No clearance required

Shock and vibration tolerance:

60 Gs for 10 milliseconds without nonrecoverable errors

Acoustical noise:

70 dB "A" scale

Inclination:

10^0 maximum

Storage and Shipping Environment

Protective packaging must be provided to protect the switch under all shipping methods (domestic and international).

Shipping temperature:

-40^0 F to 140^0 F (-40^0 C to 60^0 C)

Storage temperature:

34^0 F to 140^0 F (1^0 C to 60^0 C)

Shipping relative humidity:

5% to 100%

Storage relative humidity:

5% to 80%

Maximum wet-bulb temperature:

84^0 F (29^0 C)

Altitude:

40,000 feet (12,192 meters)

Operating Environment

Temperature:

40^0 F to 104^0 F (4^0 C to 40^0 C)

Relative humidity:

8% to 80%

Maximum wet-bulb temperature:

81^0 F (27^0 C)

Altitude:

10,000 feet (3,048 meters)

Maintenance Approach

The maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting product operation or associated applications. Fault isolation begins when one or more of the following occur:

- Event information displays at a browser-capable PC communicating with the product through the EFCM Basic Edition interface.
- Event information displays at a LAN-connected PC or workstation communicating with the rack-mount management server running a SAN management application.
- LEDs on the product front panel or FRUs illuminate to indicate a hardware malfunction.

- An unsolicited SNMP trap message is received at a management workstation, indicating an operational state change or failure.
- Event notification is received at a designated support center through an e-mail message or the call-home feature.

Fault isolation and repair information is provided through maintenance analysis procedures (MAPs). MAPs are step-by-step procedures that provide information to interpret events, isolate a failure to a FRU, remove and replace the FRU, and verify product operation. Fault isolation begins with *MAP 0000: Start MAP*.

Switch Management

The switch is managed and controlled through a:

- Customer-supplied PC platform with Internet communication to the product-resident EFCM Basic Edition interface.

  The interface allows service personnel to perform configuration tasks, view system alerts and related log information, and monitor switch status, port status, and performance. FRU status and system alert information are highly visible.

- Optional 1U management server (running a SAN management application) that provides a central point of control for up to 48 switches or managed products.

  The management server is delivered with server and client SAN management applications and the Element Manager application installed. A customer-supplied PC or workstation (with client applications installed) communicates with the server through a through a corporate intranet.

- Customer-supplied PC or UNIX-based platform with the server and client SAN management and Element Manager applications installed.

Management Server

The management server is a 1U, rack-mount unit that provides a central point of control for up to 48 connected switches or other managed products. Server applications are accessed through a LAN-attached PC or workstation with client software installed. Figure 1-3 illustrates the server with attached liquid crystal display (LCD) panel.

Figure 1-3 Management Server

The server is rack mounted in the McDATA-supplied FC-512 Fabricenter equipment cabinet. A SANpilot interface or management server is required to install, configure, and manage the switch.

The server provides two auto-detecting 10/100 Mbps Ethernet LAN connectors (RJ-45 adapters). The first adapter (LAN 1) attaches (optionally) to a public customer intranet to allow access from remote user workstations. The second adapter (LAN 2) attaches to a private LAN segment containing switches or managed products.

Management Server Specifications

This section summarizes minimum and recommended hardware specifications for the rack-mount management server. Servers may ship with more enhanced hardware, such as a faster processor, additional random-access memory (RAM), or a higher-capacity hard drive.

Minimum Specifications

Minimum server specifications are:

- 1U rack-mount server running the Intel® Pentium® 4 processor with a 2 gigahertz (GHz) or greater clock speed, using the Microsoft Windows 2000 Professional (with service pack 4), Windows XP Professional (with service pack 2), or Windows Server 2003 operating system (Enterprise Edition with service pack 1) operating system.
- TightVNC™ Viewer Version 1.2.7 client-server software control package that provides remote network access (through a web browser) to the management server desktop.
- 1,024 megabyte (MB) RAM.
- 40 gigabyte (GB) internal hard drive.
- 1.44 MB 3.5-inch slim-type disk drive.

- 24X read speed slim-type compact disk-rewritable (CD-RW) and 8X read speed digital video disk (DVD) combination drive, data only.
- 56K peripheral component interconnect (PCI) internal data and fax modem, using the V .92 dial-up specification.
- 16 MB graphics card.
- Network interface card (NIC) with two 10/100 Mbps Ethernet adapters using RJ-45 connectors.

Recommended Specifications

Recommended server specifications are:

- 1U rack-mount server running the Intel Pentium 4 processor with a 3 GHz or greater clock speed, using an 800 megahertz (MHz) front side bus, using the Microsoft Windows Server 2003 operating system (Enterprise Edition with service pack 1).
- TightVNC™ Viewer Version 1.2.7 client-server software control package that provides remote network access (through a web browser) to the management server desktop.
- 2,048 MB (or greater) double data-rate synchronous dynamic random access memory (SDRAM).
- 40 GB (or greater) internal hard drive, with advanced technology attachment (ATA-100) integrated drive electronics interface operating at 7,200 rpm.
- 1.44 MB 3.5-inch slim-type disk drive.
- 48X read speed slim-type CD-RW and 32X read speed DVD combination drive, data only.
- 56K PCI internal data and fax modem, using the V .92 dial-up specification.
- Video graphics array (VGA) capable 32 MB graphics card.
- NIC with two 10/100 Mbps Ethernet adapters using RJ-45 connectors.

Ethernet Hub (Optional)

The management server and managed switches connect through a 10/100 Base-T Ethernet hub. Figure 1-4 illustrates the 24-port hub.

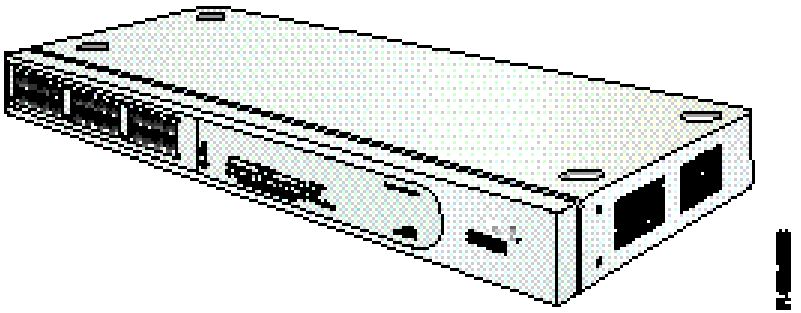


Figure 1-4 24-Port Ethernet Hub

Hubs can be daisy-chained to provide additional connections as more switches (or other McDATA managed products) are installed on a network. Multiple hubs are daisy-chained by attaching RJ-45 Ethernet patch cables and configuring each hub through a medium-dependent interface (MDI) switch.

Error-Detection, Reporting, and Serviceability Features

The switch provides the following error detection, reporting, and serviceability features:

- LEDs on switch FRUs and adjacent to Fibre Channel ports that provide visual indicators of hardware status or malfunctions.
- Redundant FRUs (SFP transceivers and power supply assemblies) that are removed or replaced without disrupting switch or Fibre Channel link operation.
- A modular design that enables quick removal and replacement of FRUs without the use of tools or equipment.
- System alerts and logs that display switch, Ethernet link, and Fibre Channel link status at the EFCM Basic Edition interface, client communicating with the management server, or customer-supplied server (running a SAN management application).
- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (loopback tests).

- An RS-232 maintenance port at the rear of the switch (port access is password protected) that enables installation or service personnel to change the switch's IP address, subnet mask, and gateway address.

  These parameters can also be changed through a Telnet session, access for which is provided through a local or remote PC with an Internet connection to the switch.

- Data collection through the EFCM Basic Edition interface or Element Manager application to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.

- Beaconing to assist service personnel in locating a specific port or switch. When port beaconing is enabled, the amber LED associated with the port flashes. When unit beaconing is enabled, the system error indicator on the front panel flashes. Beaconing does not affect port or switch operation.

- An internal modem for use by support personnel to dial-in to the management server (optional) for event notification and to perform remote diagnostics.

- Automatic notification of significant system events (to support personnel or administrators) through e-mail messages or the call-home feature.

  NOTE: The call-home feature is not available through the EFCM Basic Edition. The call-home feature may not be available if the EFCM Lite application is installed on a customer-supplied platform.

- SNMP management using the Fibre Channel Fabric Element MIB, Transmission Control Protocol/Internet Protocol (TCP/IP) MIB-II definition (RFC 1157), or a product-specific private enterprise MIB that runs on the switch. Up to six authorized management workstations can be configured through the EFCM Basic Edition interface or Element Manager application to receive unsolicited SNMP trap messages. The trap messages indicate product operational state changes and failure conditions.

- Optional SNMP management using the Fibre Alliance MIB that runs on the management server. Up to 12 authorized management workstations can be configured through the SAN

management application to receive unsolicited SNMP trap messages. The trap messages indicate operational state changes and failure conditions.

Tools and Test Equipment

This section describes tools and test equipment that may be required to install, test, service, and verify operation of the product and attached management server. These tools are supplied with the product or must be supplied by service personnel.

Tools Supplied with the Product

The following tools are supplied with the product:

- **Door key -** A door key with 5/16-inch socket (Figure 1-5) is required to open front and rear doors of the Fabricenter Equipment Cabinet. A 5/16-inch socket wrench may also be used.

Figure 1-5 Door Key

- **Loopback plug -** A multimode (shortwave laser) loopback plug (Figure 1-6) is required to perform port diagnostic tests. Loopback plugs are shipped with the product, depending on the types of port transceivers installed.

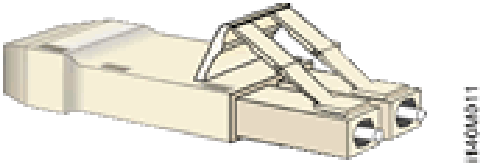


Figure 1-6 Loopback Plug

- **Fiber-optic protective plug -** For safety and port transceiver protection, fiber-optic protective plugs (Figure 1-7) are inserted in all product ports without fiber-optic cables attached. Products are shipped with protective plugs installed.

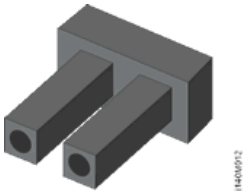


Figure 1-7 Fiber-Optic Protective Plug

- **Null modem cable -** An asynchronous RS-232 null modem cable (Figure 1-8) is required to configure product network addresses and acquire event log information through the product's serial port. The cable has nine conductors and DB-9 female connectors.

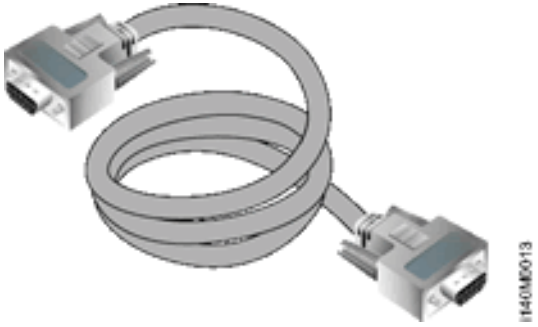


Figure 1-8 Null Modem Cable

Tools Supplied by Service Personnel

The following tools should be supplied by service personnel:

- **Scissors or pocket knife -** A sharp cutting edge (scissors or knife blade) is required to cut protective strapping when unpacking replacement FRUs.
- **Flat-tip and cross-tip (Phillips) screwdrivers -** Screwdrivers are required to remove, replace, adjust, or tighten FRUs, chassis, or cabinet components.

- **T10 Torx® tool -** The tool is required to rack-mount products or to remove, replace, adjust, or tighten chassis or cabinet components.
- **ESD grounding cable and wrist strap -** An ESD wrist strap is required when working with ESD-sensitive FRUs, including optical transceivers.
- **Maintenance terminal -** A desktop or notebook PC is required to configure product network addresses and acquire event log information through the maintenance port. The PC must have:
  - The Microsoft® Windows® 98, Windows® 2000, Windows® 2003, Windows® XP, or Windows® ME operating system installed.
  - RS-232 serial communication software (such as ProComm Plus™ or HyperTerminal) installed. HyperTerminal is provided with Windows operating systems.
- **Fiber-optic cleaning kit -** The kit contains tools and instructions to clean fiber-optic cables, connectors, loopback plugs, and protective plugs.

2 Installation Tasks

This chapter describes tasks to install, configure, and verify operation of the Sphereon 4400 Fabric Switch using the EFCM Basic Edition interface or storage area network (SAN) management application. The product can be installed on a table top, mounted in a Fabricenter equipment cabinet, or mounted in any standard 19-inch equipment rack.

Factory Defaults

Table 2-1 lists factory-set defaults for the product.

Table 2-1 Factory-Set Defaults (Product)

Item	Default
EFCM Basic Edition interface user name (case sensitive)	Administrator
EFCM Basic Edition interface password (case sensitive)	password
Customer-level password (maintenance port access)	password
Maintenance-level password (maintenance port access)	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Table 2-2 lists factory-set defaults for the rack-mount management server (running a SAN management application).

Table 2-2 Factory-Set Defaults (Management Server)

Item		Default
Liquid crystal display (LCD) front panel		9999
Windows operating system user name (case sensitive)		Administrator
Windows operating system password (case sensitive)		password
SAN management application user name (case sensitive)		Administrator
SAN management application password (case sensitive)		password
LAN 1 (public interface)	IP address	192.168.0.1
	Subnet mask	255.0.0.0
	Gateway address	0.0.0.0
LAN 2 (private interface)	IP address	10.1.1.1
	Subnet mask	255.0.0.0
	Gateway address	0.0.0.0

Installation Task Summary

Table 2-3 summarizes installation tasks for the product, optional management server, and optional Ethernet hub. The table describes each task, states if the task is optional, and lists the page reference.

Table 2-3 Installation Task Summary

Task Number and Description	Required or Optional	Page
Task 1: Verify Installation Requirements	Required.	2-4
Task 2: Unpack, Inspect, and Install the Ethernet Hub (Optional)	Perform task if hub is required to connect switch and management interface.	2-5
Task 3: Unpack, Inspect, and Install the Product	Required.	2-9
Task 4: Configure Product at the EFCM Basic Edition Interface (Optional)	Perform task if switch is managed through the EFCM Basic Edition interface.	2-12

Table 2-3 Installation Task Summary (*continued*)

Task Number and Description	Required or Optional	Page
Task 5: Configure Product Network Information (Optional)	Configure if connecting multiple switches or connecting switch and management server to a public LAN.	2-32
Task 6: Unpack, Inspect, and Install the Management Server	Required if management server is used.	2-35
Task 7: Configure Server Password and Network Addresses	Required if management server is used.	2-38
Task 8: Configure Management Server Information	Required if management server is used.	2-40
Task 9: Configure Windows Operating System Users	Required if management server is used.	2-44
Task 10: Set Management Server Date and Time	Required if management server is used.	2-46
Task 11: Configure the Call-Home Feature (Optional)	Configure if specified by customer and telephone connection is provided.	2-48
Task 12: Assign User Names and Passwords	Required if management server is used.	2-49
Task 13: Configure the Product to the Management Application	Required if management server is used.	2-51
Task 14: Record or Verify Server Restore Information	Required if management server is used.	2-52
Task 15: Verify Product-to-Server Communication	Required if management server is used.	2-53
Task 16: Configure PFE Key (Optional)	Configure if product feature enablement (PFE) key is ordered.	2-55
Task 17: Configure Management Server (Optional)	Configure for open-systems host control of switch.	2-56
Task 18: Set Product Date and Time	Required if management server is used.	2-57
Task 19: Configure the Element Manager Application	Required if management server is used.	2-59
Task 20: Back Up Configuration Data	Required if management server is used.	2-75
Task 21: Cable Fibre Channel Ports	Required.	2-77
Task 22: Configure Zoning (Optional)	Perform task to configure zoning.	2-78
Task 23: Connect Product to a Fabric Element (Optional)	Perform task to connect switch to a Fibre channel fabric.	2-79
Task 24: Register with the McDATA Filecenter	Required.	2-80

Task 1: Verify Installation Requirements

Ensure that the following requirements are met prior to product and management interface installation. Ensure:

- A site plan is prepared, configuration planning tasks are complete, planning considerations are evaluated, and related planning checklists are complete. Refer to *McDATA Products in a SAN Environment - Planning Manual* (620-000124) for information.
- Fibre Channel SAN design and director, fabric switch, and SAN router device connectivity are evaluated, and the related planning worksheet is complete. Refer to the *McDATA Products in a SAN Environment - Planning Manual* (620-000124) for information.
- Support is available for one of the following product management methods:
  - — A browser-capable PC and Internet connectivity to support the product-resident EFCM Basic Edition interface, or
  - — A rack-mount management server or browser-capable PC and LAN segment connectivity to support operation of SAN management and Element Manager applications.
- Support equipment and technical personnel are available for the installation.
- The required number and type of fiber-optic jumper cables are delivered and available. Ensure that the cables are of the correct length and have the required connectors.
- A Fabricenter cabinet or customer-supplied 19-inch equipment rack and associated hardware are available (optional).
- Remote workstations or simple network management protocol (SNMP) workstations are available (optional).
- Workstations are customer-supplied and connected through a public or dedicated LAN segment.

Task 2: Unpack, Inspect, and Install the Ethernet Hub (Optional)

This section describes how to unpack, inspect and install the theernet hub.

The product is managed through either:

- An Internet connection to a browser-capable PC (EFCM Basic Edition interface). Connection of a LAN segment with multiple switches to the Internet may require installation of a 24-port Ethernet hub.
- A 10/100 megabit per second (Mbps) LAN connection to a management server. Connectivity may require installation of a 24-port Ethernet hub. A combination of up to 48 products can be configured and managed on one network, therefore multiple, daisy-chained hubs may be required to provide sufficient port connections.

The following paragraphs provide instructions to unpack, inspect, and install one or more Ethernet hubs.

- If the existing Ethernet LAN segment is adequate for connectivity and a hub is not delivered, this task is not required. Go to *Task 3: Unpack, Inspect, and Install the Product*.
- If the hub is delivered in a Fabricenter equipment cabinet, go to *Task 5: Configure Product Network Information (Optional)*.

Unpack and Inspect Ethernet Hub

To unpack and inspect Ethernet hub(s) use the following steps:

1. Inspect shipping container(s) for damage. Ensure a freight carrier representative is present when the container is opened. Unpack shipping container(s) and inspect each item for damage. Ensure that the packaged items correspond to items listed on the enclosed bill of materials.
2. Contact the solution center if items are damaged or missing,:

   Phone: (800) 752-4572 or (720) 558-3910

   Fax: (720) 558-3851

   E-mail: support@mcdata.com

Desktop Installation

To install and configure up to three Ethernet hubs on a desktop, use the following steps:

1. Remove the backing from the four adhesive rubber pads and apply the pads to the underside of each hub. Ensure that the pads are aligned with the scribed circles at each corner.
2. Position the first hub on a table or desktop as directed by the customer.
3. Stack the remaining hubs on top of the first hub. Ensure that the adhesive rubber pads on the underside of a hub align with the recesses on the top of the hub below.
4. Daisy-chain (connect) the hubs using the following steps:
   a. **Connect the top and middle stacked hubs**, connect an RJ-45 patch cable to port **24** of the top hub, then connect the cable to port **12** of the middle hub.
   b. **Connect the bottom and middle stacked hubs**, connect a second RJ-45 patch cable to port **24** of the middle hub, then connect the cable to port **12** of the bottom hub.
   c. Use a pointed instrument to set the medium-dependent interface (MDI) switch on the top and middle hubs to **MDI** (in) as shown in Figure 2-1 (**1** and **2**).
   d. Set the medium-dependant interface (MDI) switch on the bottom hub to **MDIX** (out) as shown in Figure 2-1 (**3**).

NOTE: To connect two hubs, use step b and step c (middle and bottom hub instructions only).

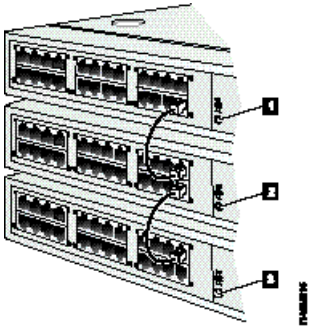


Figure 2-1 **Patch Cable and MDI Selector Configuration**

5. Connect a power cord to an AC power strip and the receptacle at the rear of each hub. Use an extension cord if required.
6. Connect the AC power strip to facility power. Power for each hub switches on when the strip is connected to facility AC power.
7. Inspect the front panel of each hub. Ensure that each green **Power** light-emitting diode (LED) illuminates.

Rack-Mount Installation

You will need a pointed instrument (pencil tip or bent paper clip), #2 Phillips screwdriver, and 1/8-inch Allen wrench for this procedure.

To install and configure up to three Ethernet hubs in a Fabricenter cabinet or customer-supplied 19-inch equipment rack, use the following steps

1. Secure one mounting bracket to each side of the first hub as shown in Figure 2-2. Use the two brackets and four pan-head Phillips screws (8/32 x 0.5-inch) provided.

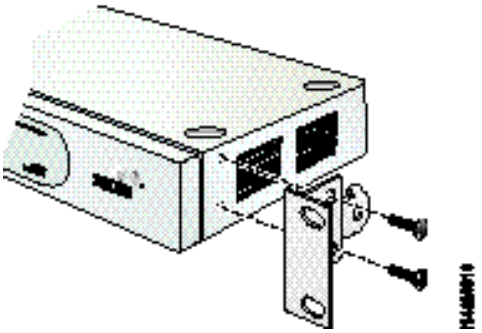


Figure 2-2 Mounting Bracket Installation (Ethernet Hub)

2. Position the hub as directed by the customer. Align screw holes in the mounting brackets with screw holes in the rack-mount standards.
3. Secure both sides of the hub to the rack-mount standards. Use the 1/8-inch Allen wrench and four Allen-head mounting screws (10/32 x 0.5-inch) provided.
4. Repeat step 1 through step 3 for the remaining hubs.
5. Daisy-chain (connect) the hubs using the following procedure:
   a. **Connect the top and middle stacked hubs,** connect an RJ-45 patch cable to port **24** of the top hub, then connect the cable to port **12** of the middle hub.
   b. **Connect the bottom and middle stacked hubs**, connect a second RJ-45 patch cable to port **24** of the middle hub, then connect the cable to port **12** of the bottom hub.
   c. Use a pointed instrument Figure 2-1 (**1** and **2**), to set the medium-dependent interface (MDI) switch on the top and middle hubs to **MDI** (in). As shown in Figure 2-1 (**3**), set the MDI switch on the bottom hub to **MDIX** (out).

   NOTE: To connect two hubs follow the middle and bottom hub instructions only.

6. Connect a power cord to a rack power strip and the receptacle at the rear of each hub. Power for each hub switches on when the hub (and equipment rack) are connected to facility AC power.

NOTE: Ensure each hub is connected to a separate rack power strip.

7. Inspect the front panel of each hub. Ensure each green **Power** LED illuminates.

Task 3: Unpack, Inspect, and Install the Product

Follow the procedures in this section to unpack, inspect, and install one or more switches. If the switch is delivered in a Fabricenter equipment cabinet, go to *Task 5: Configure Product Network Information (Optional)*.

Unpack and Inspect Switch

To unpack and inspect switch(es), use the following steps:

1. Inspect shipping container(s) for damage. Ensure that a freight carrier representative is present when the container is opened. Unpack shipping container(s) and inspect each item for damage. Ensure that the packaged items correspond to items listed on the enclosed bill of materials.
2. Contact the technical support center if any tems are damaged or missing,:

   Phone: (800) 752-4572 or (720) 558-3910

   Fax: (720) 558-3851

   E-mail: support@mcdata.com

Desktop Installation

To install a switch on a desktop, use the following steps:

1. Remove the backing from the three adhesive rubber pads and apply the pads to the underside of the switch. Ensure pads are aligned with the scribed circles.
2. Position the switch on a table or desktop as directed by the customer. Ensure:

   — Grounded AC electrical outlets are available.

   — Adequate ventilation is present, and areas with excessive heat, dust, or moisture are avoided.

— All planning considerations are met. Refer to *McDATA Products in a SAN Environment - Planning Manual* (620-000124) for information.

3. Ensure that all field-replaceable units (FRUs) are installed as ordered.
4. Connect power supply adapter cords to threaded output jacks at the rear of the chassis (second external power supply is optional). Twist the cord clockwise to lock and secure the connection.
5. Connect AC power cords to connectors on each external power supply and to separate (for redundancy) facility power sources that provide single-phase, 100 to 240 volt alternating current (VAC) current.

   When the first power cord is connected, the switch powers on and performs power-on self-tests (POSTs). During POSTs:

   a. The green power (**PWR**) LED on the front panel illuminates.
   b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.
   c. The green LED associated with the Ethernet port blinks momentarily while the port is tested.
   d. LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.

   After successful POST completion, the **PWR** LED remains illuminated and all other front panel LEDs extinguish.

   If a POST error or other malfunction occurs, go to *MAP 0000: Start MAP* to isolate the problem.
6. Perform one of the following:

   — If the switch is to be managed through the EFCM Basic Edition interface, go to *Task 4: Configure Product at the EFCM Basic Edition Interface (Optional)*.

   — If the switch is to be managed through a management or customer-supplied server, go to *Task 5: Configure Product Network Information (Optional)*.

Rack-Mount Installation

You will need an optional rack-mount kit, T10 Torx tool, and #2 Phillips screwdriver for this procedure.

To install and configure the switch in a Fabricenter cabinet or a customer-supplied equipment rack, use the following steps:

1. Locate the rack-mount position as directed by the customer. The switch is 1.75 inches, or 1U high.
2. Ensure that all FRUs are installed as ordered.
3. Open the rack-mount kit and inspect the contents. Refer to the enclosed bill of materials and verify all parts are delivered.
4. Install the switch and optional slide tray (holds two switches) in the equipment cabinet. Refer to *McDATA Sphereon 4400 Switch Rack-Mount Kit Installation Instructions* (958-000480) for guidance.
5. Connect power supply adapter cords to threaded output jacks at the rear of the chassis (second external power supply is optional). Twist the cord clockwise to lock and secure the connection.
6. Connect AC power cords to connectors on each external power supply and to separate (for redundancy) rack power strips connected to a facility power source that provides single-phase, 100 to 240 VAC current.

   When the first power cord is connected, the switch powers on and performs POSTs. During POSTs:

   a. The green power (**PWR**) LED on the front panel illuminates.
   b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.
   c. The green LED associated with the Ethernet port blinks momentarily while the port is tested.
   d. LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.

   After successful POST completion, the **PWR** LED remains illuminated and all other front panel LEDs extinguish.

   If a POST error or other malfunction occurs, go to *MAP 0000: Start MAP* to isolate the problem.
7. Perform one of the following:

— If the switch is to be managed through the EFCM Basic Edition interface, go to *Task 4: Configure Product at the EFCM Basic Edition Interface (Optional)*.

— If the switch is to be managed through a management or customer-supplied server, go to *Task 5: Configure Product Network Information (Optional)*.

Task 4: Configure Product at the EFCM Basic Edition Interface (Optional)

Follow the procedures in this section to configure the product from the EFCM Basic Edition interface. A browser-capable PC with Internet or Ethernet LAN access is required. To open the interface, use the following steps:

1. Connect the Ethernet patch cable (supplied with the product) to the RJ-45 connector (labelled **10/100**) at the front panel.
2. Connect the remaining end of the Ethernet cable to the Internet or LAN segment as directed by the customer. If the hub installed in *Task 2: Unpack, Inspect, and Install the Ethernet Hub (Optional)* provides connectivity, connect the cable to any available hub port.
3. Open the browser application (Netscape Navigator or Internet Explorer).
4. Enter the default Internet Protocol (IP) address of the switch (**10.1.1.10**). The *Enter Network Password* dialog box appears.
5. Type the case-sensitive default user name (**Administrator**) and password (**password**) and click *OK*. The *First Time Login View* appears.
6. Type customer-specified values in the *User Name*, *New Password*, and *Confirm Password* fields, then click *Activate*. The *Topology View* appears with status information about each fabric element, including the product to be configured.
7. Click *Switch Details*. The *Hardware View* appears (Figure 2-3).

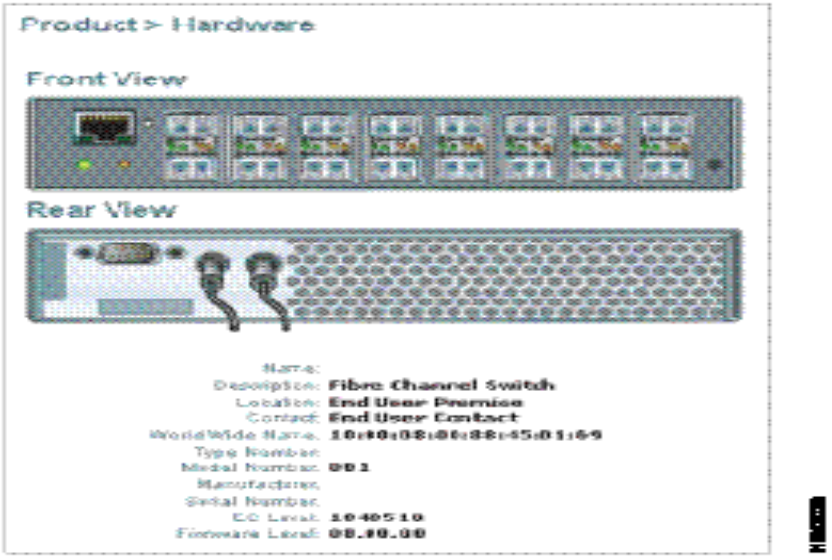


Figure 2-3 Hardware View

8. S electively perform the following tasks to configure the product from the EFCM Basic Edition interface, according to customer requirements:

Product	• Identification • Date and time • Parameters • Fabric parameters • Network addresses.
Ports	• Basic information • Buffer-to-buffer credits (BB_Credits) • N_Port identifier virtualization (NPIV).
Management	• SNMP trap message recipients • Command line interface (CLI) • Open systems management server (OSMS) • Secure socket layer (SSL) encryption.

Options	Product feature enablement (PFE) keys.
Security	• SANtegrity authentication (settings, access control list, and remote authentication dial-in user service (RADIUS) server support), • Enterprise Fabric Mode • SANtegrity binding (fabric, switch, and port binding
Interswitch Links	• OpenTrunking • Preferred path, and • Interswitch link (ISL) port fencing

Configure Product Identification

Follow the procedures in this section to configure the product identification.

NOTE: The *Name*, *Location*, and *Contact* variables correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*, and are used by management workstations when obtaining product data.

1. Select *Identification* from the *Configure* menu (*Configure>Switch>Identification*). The *Identification View* appears (Figure 2-4).

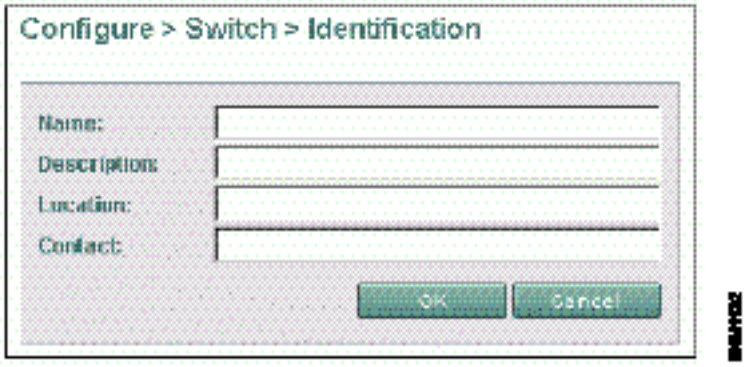


Figure 2-4 Identification View

   a. Type a unique product name of 24 alphanumeric characters or less in the *Name* field. If installed on a public LAN, the name should reflect the product's Ethernet network domain name system (DNS) host name.

b. Type a product description of 255 alphanumeric characters or less in the *Description* field.

c. Type the product's physical location (255 alphanumeric characters or less) in the *Location* field.

d. Type the name of a contact person (255 alphanumeric characters or less) in the *Contact* field.

2. Click *OK* to save and activate changes.

Configure Date and Time

To configure product date and time, use the following steps:

1. Select *Date & Time* from the *Configure* menu (*Configure>Switch>Date & Time*). The *Date Time View* appears (Figure 2-5).

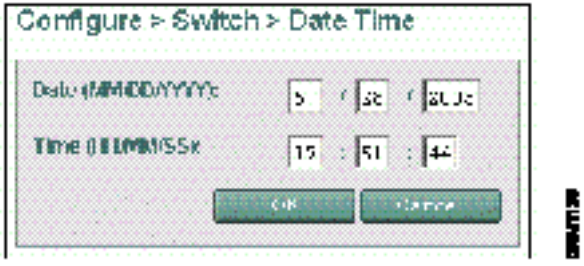


Figure 2-5 Date Time View

a. Configure the Date using the *Date* field:

- Month (*MM*): **1** - **12**.
- Day (*DD*): **1** - **31**.
- Year (*YYYY*): greater than **1980**.

b. Configure the Time using the *Date* field:

- Hour (*HH*): **0** -**23**.
- Minute (*MM*): **0** - **59**.
- Second (*SS*): **0** - **59**.

2. Click *OK* to save and activate changes.

Configure Parameters

To configure product operating parameters, use the following steps:

1. Set the product offline. Refer to *Setting Online State* for instructions.
2. Select *Parameters* from the *Configure* menu (*Configure>Switch>Parameters*). The *Parameters View* appears (Figure 2-6).
   a. Select the *Domain ID Offset* value from the drop-down list. Values available in the drop-down list are 0, 32, 64, 96 (default), 128, 160, and 192. Domain IDs minus the offset are still in the 1-31 range.

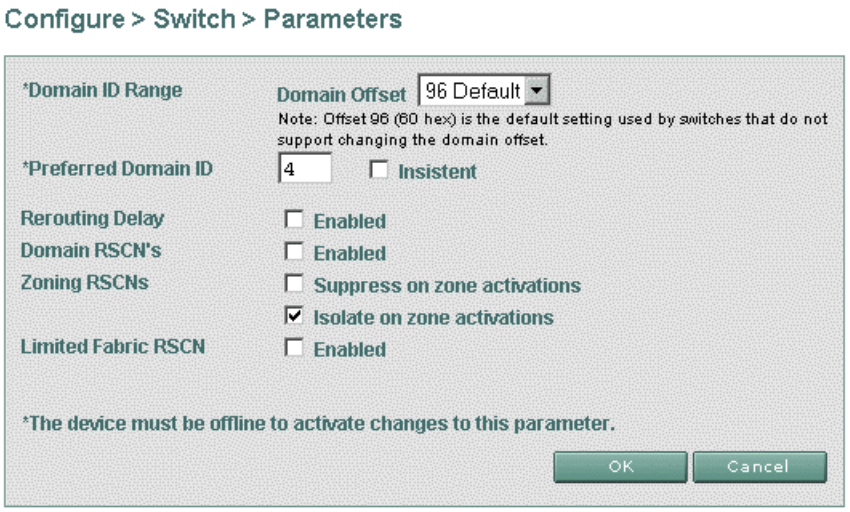


Figure 2-6 Parameters View

   b. Type a value (1-31) in the *Preferred Domain ID* field.
   c. Enable (check) the *Insistent Domain ID* field if you want the *Preferred Domain ID* to become the active domain ID when the fabric initializes.
   d. Enable (check) the *Rerouting Delay* field if you want the traffic to be delayed through the fabric by the error detect time out value (E_D_TOV). This delay ensures that the Fibre Channel frames are delivered to their destination in order.

e. Enable (check) the *Domain RSCN* field, if you want the attached devices to register and receive notification when other devices change state.

f. Enable (check) the *Suppress RSCN on Zone Set Activations* if you do not want the RSCNs to be transmitted when a zone set is activated.

g. Enable (check) the *Isolate on zone activations* field if you want only devices that require RSCN notification due to a zoning configuration change to receive RSCNs. Do not enable this option if *Suppress on zone set activations* is enabled because RSCNs will not be sent to attached devices.

h. Enable (check) the *Limited Fabric RSCN* field if you do not want the RSCNs to be transmitted after a switch initial program load (IPL).

i. Enable (check) the Node port virtualization to assign multiple Fibre Channel addresses to a single N_Port port.

3. Click *OK* to save and activate changes.
4. Set the product online. Refer to *Setting Online State* for instructions.

Configure Fabric Parameters

To configure fabric operating parameters, use the following steps.

1. Set the product offline. Refer to *Setting Online State* for instructions.
2. Select *Fabric Parameters* from the *Configure* menu (*Configure>Switch>Fabric Parameters*). The *Fabric Parameters View* appears (Figure 2-7).

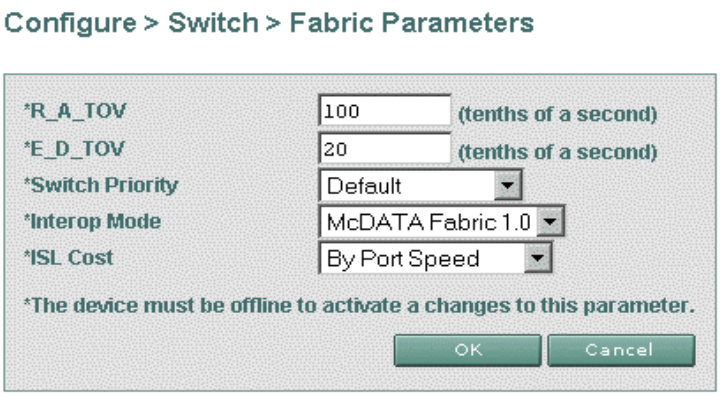


Figure 2-7 Fabric Parameters View

a. Type a value between **10 - 1200** tenths of a second (1 - 120 seconds) in the *R_A_TOV* field. Ten seconds (**100**) is the recommended value. The R_A_TOV value must exceed the E_D_TOV value.

b. Type a value between **2** - **600** tenths of a second (0.2 - 60 seconds) at the *E_D_TOV* field. Two seconds (**20**) is the recommended value.

NOTE: Fabric elements must be set to the same R_A_TOV and E_D_TOV values. An ISL between fabric elements with different values segments and prevents communication.

---

c. Select from the *Switch Priority* drop-down list to designate the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself). Available selections are *Default*, *Principal*, and *Never Principal*.

Principal is the highest priority setting, *Default* is next, and *Never Principal* is the lowest. At least one switch in a fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all ISLs segment.

d. Select from the *Interop Mode* drop-down list to set the product operating mode. This setting affects the management mode and does not affect port operation. Available selections are:

- **McDATA Fabric 1.0 -** Select this option if the product is fabric-attached only to other McDATA directors or switches operating in McDATA fabric mode.
- **Open Fabric 1.0 -** Select this option (default) for managing heterogeneous fabrics and if the product is fabric-attached to McDATA directors or switches and other open-fabric compliant switches.

NOTE: With Open Fabric 1.0 enabled, the default zone set is disabled.

e. Select from the *ISL Cost Configuration* drop-down list, to select By Port Speed or Ignore Port Speed to calculate fabric shortest path first (FSPF) cost.

3. Click *OK* to save and activate changes.
4. Set the product online. Refer to *Setting Online State* for instructions.

Configure Network Information

Follow the procedure in this section to configure the network information.

Ensure the LAN installation with the network administrator:

- If one product is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require any change.
- Multiple products are installed or a public LAN segment is used, network information must be changed to conform to the LAN addressing scheme.

To change product network information, use the following steps:

1. Select *Network* from the *Configure* menu (*Configure>Switch>Network*). The *Network View* appears (Figure 2-8).

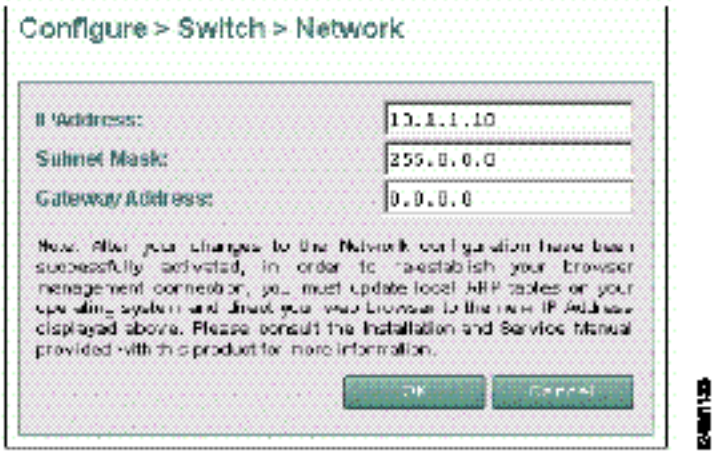


Figure 2-8 Network View

a. Type a value in the *IP Address* field (default is **10.1.1.10**).

b. Type a value in the *Subnet Mask* field (default is **255.0.0.0**).

c. Type a value in the *Gateway Address* field (default is **0.0.0.0**).

2. Click *OK* to save and activate changes.

   An acknowledgement message appears, indicating the browser PC must be directed to the new IP address.

3. Update the address resolution protocol (ARP) table for the browser PC.

   a. Close the EFCM Basic Edition interface and all browser applications.

   b. Open the command prompt (DOS) on your Windows desktop.

   c. Delete the switch's ***old*** IP address from the ARP table. At the command (**C:**) prompt, type **arp -d** ***xxx.xxx.xxx.xxx***, where ***xxx.xxx.xxx.xxx*** is the old IP address for the switch.

   d. Close the command prompt window and return to the Windows desktop.

4. Perform a power-on reset (POR) (*IML or Reset Switch*).

5. Open the browser (Internet Explorer or Netscape Navigator) on your PC. Enter the ***new*** IP address of the product as the URL. The *Enter Network Password* dialog box appears.

6. Type the case-sensitive user name and password and click *OK*. The *EFCM Basic Edition* interface appears with the *Topology View* displaying the status information about each fabric element.

Configure Basic Port Information

To configure basic port information, use the following steps:

1. Select *Basic Info* from the *Configure* menu (*Configure>Ports>Basic Info*). The *Basic Information View* appears(Figure 2-9).
   a. Type a port name (24 alphanumeric characters or less) for each port to be configured in the *Name* field. The port name should characterize the device to which the port is attached.
   b. Enable the check box in the *Blocked* column if you want to block a port (default is unblocked).
   c. Disable the check box in the *Fabric Address Notify* column if you want to disable the feature (default is enabled). When enabled, an FL_Port transmits FAN frames after loop initialization to ensure that FC-AL devices are still logged in.

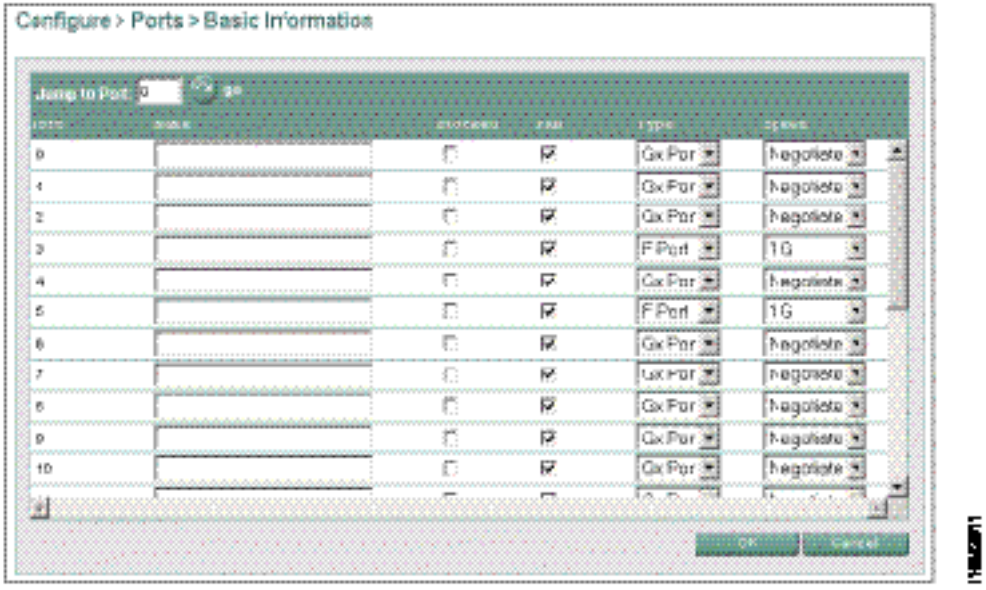


Figure 2-9 Basic Information View

d. Select an option from the drop-down list in the *Port Type* column to configure the port type. The available options are fabric port (**F**), expansion port (**E**), generic port (**G**), generic mixed port (**GX**), and fabric mixed port (**FX**).

e. Select an option from the drop-down list in the *Speed (Gb/s)* column to configure the port transmission rate. The available options are auto-negotiate between speeds (**Negotiate**), 1.0625 gigabit per second (Gbps) operation (**1 Gb/sec**), 2.1250 Gbps operation (**2 Gb/sec**), and 4.2500 Gbps operation (**4 Gb/sec**).

2. Click *OK* to save and activate changes.

Configure Port BB_Credit

Follow the procedure in this section to configure a port to receive BB_Credit.

The switch provides a port buffer pool of 150 receive BB_Credits. Each port can be assigned between two and 120 credits, provided the total credits allocated to all ports does not exceed 150. The default value is six credits per port.

To configure ports to receive BB_Credit, use the following steps:

1. Set all or a subset of user-specified ports offline. Refer to *Setting Online State* or *Blocking or Unblocking a Port* for instructions.
2. Select *Ports* and *RX BB_Credit* from the *Configure* menu at any view. The *RX BB_Credit View* appears.
3. Perform one of the following:
   - To set all offline ports to default values, click *Default*.
   - To set an offline port to a user-specified value, type the desired value in the *RX BB_Credit* column.
4. Click *OK* to save and activate changes.
5. Set ports online. Refer to *Setting Online State* (all) or *Blocking or Unblocking a Port* (specified ports) for instructions.

Configure Port NPIV

NPIV allows multiple (up to 256) Fibre Channel addresses to be assigned to a node (N_Port). The NPIV feature must be installed. Refer to *Installing PFE Keys (Optional)* for instructions.

To configure port NPIV, use the following steps:

1. Select *NPIV* from the *Configure* menu (*Configure>Ports>NPIV*). The *NPIV View* appears.
2. Click *Enable* to activate NPIV operation for the product.
3. Type a desired value(**1** through **256**) in the *Login* column.
4. Click *OK* to save and activate changes.

Configure SNMP

Follow the procedure in this section to configure names, write authorizations, addresses, and user datagram protocol (UDP) port numbers for SNMP trap message recipients.

To configure recipient workstations, use the following steps:

1. Select *SNMP* from the *Configure* menu (*Configure>SNMP*). The *SNMP View* appears (Figure 2-10).
   a. Click *Enable* to activate the installed SNMP agent.
   b. Select the appropriate Fibre Alliance management information base (FA MIB) from the *FA MIB Version* drop-down list. Valid selections are **FA MIB Version 3.0** or **FA MIB Version 3.1**.

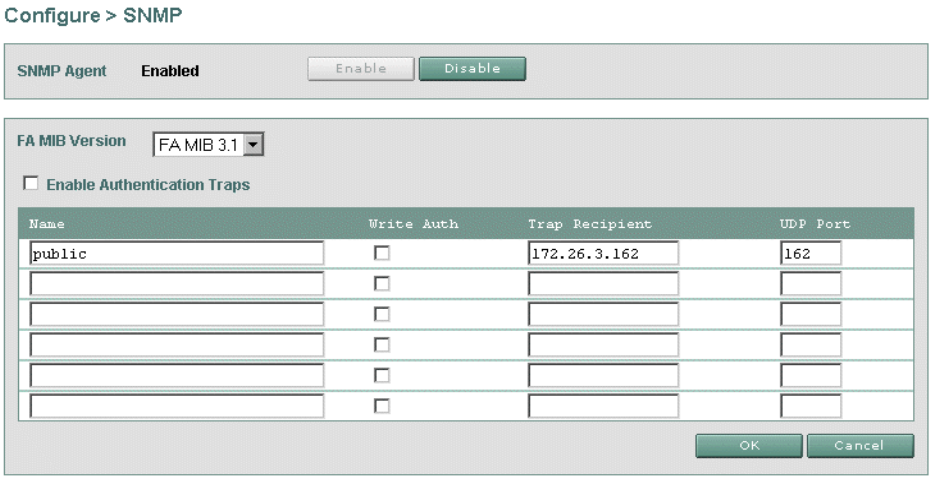


Figure 2-10 SNMP View

   c. Check the *Enable Authentication Traps* check box to enable transmission of SNMP trap messages to recipients.

d. Type a community name, for each configured recipient (32 alphanumeric characters or less) in the *Name* field. The name is incorporated in SNMP trap messages to ensure against unauthorized viewing.

e. Check the box in the *Write Auth* column to enable write authorization for the trap recipient (default is disabled). When enabled, a configured user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.

f. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the *Trap Recipient* field. It is recommended that the IP address be used.

g. Type a decimal port number in the *UDP Port Number* field to specify the UDP port number.

2. Click *OK* to save and activate changes.

Enable CLI

Follow the procedure in this section to toggle (enable or disable) the state of the product's command line interface. To change the CLI state, Enable the check box *Enable CLI* from the *Configure* menu

Enable or Disable the CLI for SSH

To configure SSH, Select Configure > SSH on the navigation panel. The SSH configuration page (Figure 2-11) appears.

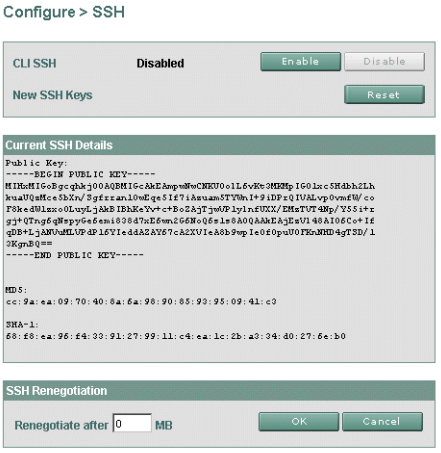


Figure 2-11 SSH Configuration

Click Enable to enable SSH. Click Disable to disable the SSH. When SSH is enabled, only SSH is allowed, and all data sent over the connection is encrypted. When the SSH is disabled, only Telnet is allowed, and the data is not encrypted.

Enable or Disable Host Control

Folllow the procedure in this section to configure the open systems management server and enable OSI host control of the product. Implementing and enabling OSI host control requires installation of a SAN management application on the OSI server. Applications include Veritas® SANPoint™ Control or Tivoli® NetView®.

To enable or disable OSMS host control:, use the following steps

Open Systems Only

1. Select *OSMS* from the *Configure* menu (*Configure>OSMS*). The *OSMS View* appears (Figure 2-12).

Figure 2-12 OSMS View

2. Perform one of the following:
   - Click *Enable* to activate OSMS.
   - Click *Disable* to deactivate OSMS.
3. Click the *Enable Host Control* check box to activate host control of the product.
4. Click *OK* to save and activate changes.

Configure SSL Encryption

SSL is a protocol that encrypts internet communications. The protocol uses key encryption and includes a digital certificate that enables server authentication and SSL session initialization.

To configure SSL encryption, use the following steps:

1. Select *SSL* from the *Configure* menu (*Configure>SSL*). The *SSL View* appears (Figure 2-13).
2. Perform one of the following:
   - Click *Enable* to activate web SSL.
   - Click *Disable* to deactivate web SSL.
3. Perform one of the following:
   - Click *Enable* to activate software SSL.
   - Click *Disable* to deactivate software SSL.

Figure 2-13 SSL View

4. Type a value between **30** and **3650** in the *Expires in* field to define the expiration period (in days) of the digital certificate. The default is **365** days.
5. Click *Generate* to generate a new certificate.
6. Type a value between **50** and **10000** in the *Renegotiate after* field to define a renegotiation parameter (in megabytes) for the SSL session key.
7. Click *OK* to save and activate changes.

Installing PFE Keys (Optional)

Follow the procedures in this section to install optional features using PFE keys.

After purchasing a feature, you must obtain the PFE key by following the enclosed instructions. The key is an alphanumeric string consisting of uppercase and lowercase characters that must be entered exactly, including dashes. An example format is:

XxXx-XXxX-xxXX-xX.

Keys are encoded to work only with the serial number of the installed product. Note down the key. This will help you to re-install the feature when required.

If the product fails and is replaced, obtain new PFE keys from the technical support center (**800-752-4572** or **support@mcdata.com**). You will have to provide the serial numbers of the failed and replacement products, and the old PFE key number or transaction code.

The optional features you can install using PFE-keys are listed below:

- **Element Manager application -** This feature enables out-of-band product management through an Element Manager interface. Products are delivered with the application enabled for a 31-day grace period. Before grace period expiration, the application must be reactivated through a PFE key.
- **Flexport Technology -** A Flexport Technology product is delivered at a discount without all Fibre Channel ports enabled. When additional port capacity is required, the remaining ports are incrementally enabled through this feature.
- **Full volatility -** This feature ensures no Fibre Channel frames are stored after the product is powered off or fails, and a memory dump file (that possibly includes classified data frames) is not included as part of the data collection procedure.
- **N_Port ID virtualization -** This feature allows up to 256 Fibre Channel addresses to be assigned to an N_Port.
- **OpenTrunking -** This feature provides dynamic load balancing of Fibre Channel traffic across multiple ISLs.
- **SANtegrity (enhanced) -** This feature enhances security in SANs by combining the functions of SANtegrity authentication (restricting access to Fibre Channel elements) and SANtegrity binding (controlling large and mixed fabrics).

To install the optional features using EFCM Basic, use the following steps:

1. Select *Optional Features* from the *Configure* menu (*Configure>Optional Features*) ***or*** *Security* menu (*Security>Optional Features*). The *Maintenance Feature Installation View* appears (Figure 2-14).

   Feature status is indicated by a green check mark ✔ (installed) or a red X (uninstalled). Flexport Technology status is indicated by the number of installed ports. Click a feature title in the *Feature* panel and a description appears in the *Feature Details* panel.

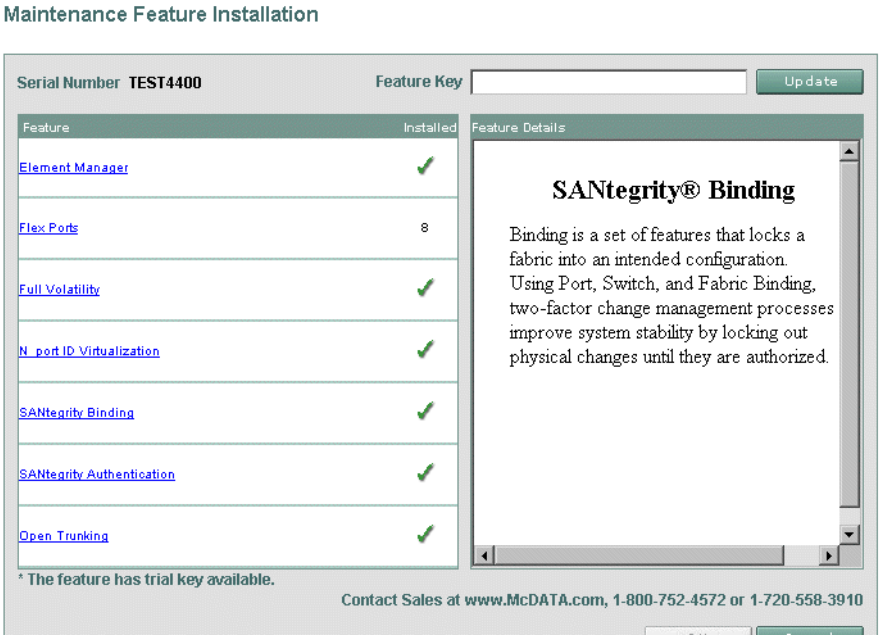

Maintenance Feature Installation
Serial Number TEST4400
Feature Key
Update
Feature
Installed
Feature Details
Element Manager
Flex Ports
8
Full Volatility
N_port ID Virtualization
SANtegrity Binding
SANtegrity Authentication
Open Trunking
SANtegrity® Binding
Binding is a set of features that locks a fabric into an intended configuration. Using Port, Switch, and Fabric Binding, two-factor change management processes improve system stability by locking out physical changes until they are authorized.
* The feature has trial key available.
Contact Sales at www.McDATA.com, 1-800-752-4572 or 1-720-558-3910

Figure 2-14 Maintenance Feature Installation View

2. Type the key in the *Feature Key* field and click *Update*. The interface refreshes and indicates the update changes in the *Feature* panel.

   NOTE: When *OK* is selected, all features are updated with new features.

3. Click *OK*. New PFE key(s) activate, the message **Feature installation in process. Your browser connection will be unavailable until unit restart is complete.** appears, and the product performs a non-disruptive (to Fibre Channel traffic) firmware reset.

   After the product reset, the message **Feature installation complete. Click here to login.** appears.

4. Click **here** to login and start a new EFCM Basic Edition session. The *Enter Network Password* dialog box appears.

Configure Security

This section describes the security features for the product that may be optionally configured.

NOTE: The enhanced SANtegrity PFE key (SANtegrity authentication and SANtegrity binding) must be installed (*Installing PFE Keys (Optional)*) to configure these features.

Select *Security* from the configrue menu *(Configure>Security)* and choose from one of the following options in the drop-down menu:

- **Authentication settings -** The *Authentication Settings View* provides four pages to configure optional SANtegrity authentication features, including:
  - **User settings -** Configure password-protected administrator and operator access to the EFCM Basic Edition and command line interfaces.
  - **Software settings -** Configure challenge handshake authentication protocol (CHAP) controlled management interface access (out-of-band and inband) to the product.
  - **Device settings -** Configure a CHAP secret authentication sequence for nodes (devices) attached to the product through E_Ports or N_ports.
  - **Port settings -** Override product-level authentication settings and enable or disable device communication on a per-port basis.
- **IP Access control list -** Use the *IP Access Control List View* to configure a list of device IP addresses or a range of device IP addresses authorized to communicate with the product.

- **RADIUS - U**se the *RADIUS Server View* to configure up to three remote authentication dial-in user service (RADIUS) servers as part of SANtegrity authentication. A RADIUS server stores and authenticates passwords and CHAP secrets.
- **Enterprise Fabric Mode -** Use the *Enterprise Fabric Mode View* to enable or disable Enterprise Fabric Mode (EFM). Fabric binding is activated when EFM is enabled.
- **Fabric binding -** Use the *Fabric Binding View* to lock parameters of a fabric in accordance with the user configuration. Fabric binding creates a membership list of element (director or switch) Domain_IDs and worldwide names (WWNs) that can communicate with the product.
- **Switch binding -** Use the *Switch Binding View* to create a membership list of node (device) WWNs that can attach to the product. The specified connection policy restricts product access through E_Ports, F_Ports, or in general (all ports).
- **Port binding -** Use the *Port Binding View* to bind an attached device WWN to a product Fibre Channel port.

To configure optional features, refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.

Configure Interswitch Links

This section describes the procedures to configure the optional ISL performance features enabled through *Configure* menu selections. The OpenTrunking feature requires PFE key installation. Refer to *Installing PFE Keys (Optional)* for instructions. Features include:

- **OpenTrunking (*Configure>Performance>Open Trunking*)-** Use the *OpenTrunking View* to optimize ISL bandwidth. The feature monitors data rates (congestion and BB_Credit starvation) through multiple ISLs and load balances traffic (from congested to uncongested links) accordingly.
- **Preferred path (*Configure>Performance>Preferred path)* -** Use the *Preferred Path View* to specify and configure one or more ISL data paths between multiple fabric elements. At each fabric element, a preferred path consists of a source port, exit port, and destination Domain_ID.

- **Port fencing (*Configure>Performance>Port fencing*)-** Use the *Port Fencing View* to minimize ISLs that bounce (repeatedly attempt to establish a connection), causing disruptive fabric rebuilds. Fencing defines a bounce threshold that when reached, automatically blocks the disruptive E_Port.

To configure features, refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions. If no additional options or features are to be configured, go to *Task 21: Cable Fibre Channel Ports*.

Task 5: Configure Product Network Information (Optional)

Follow the procedures in this section to configure product network information:

- **MAC address -** The media access control (MAC) address is programmed into FLASH memory on the control processor (CTP) card at manufacture. The MAC address is unique for each product, and should not be changed.
- **IP address -** The default IP address is **10.1.1.10**. If multiple products are installed on the same LAN, each product (and the management server) must have a unique IP address.

NOTE: If multiple products and the management server are delivered in a Fabricenter equipment cabinet, all devices are configured with unique IP addresses that do not require change. The addresses require change only if multiple cabinets are LAN-connected.

- **Subnet mask -** The default subnet mask is **255.0.0.0**. If the product is installed on a complex public LAN with one or more routers, the address may require change.
- **Gateway address -** The default gateway address is **0.0.0.0**. If the product is installed on a public LAN, the gateway address must be changed to the address of the corporate intranet's local router.

Ensure that the LAN installation with the customer.

- If one product is installed on a dedicated LAN, network addresses do not require change. Go to *Task 6: Unpack, Inspect, and Install the Management Server*.
- If multiple products are installed or a public LAN segment is used, network addresses must be changed to conform to the customer's LAN addressing scheme.

Perform the following steps to change a product IP address, subnet mask, or gateway address.

NOTE: An asynchronous RS-232 modem cable and maintenance terminal (desktop or notebook PC) with a Windows-based operating system and RS-232 serial communication software (such as ProComm Plus or HyperTerminal) are required.

1. Use a Phillips screwdriver to remove the protective cap from the 9-pin maintenance port at the rear of the chassis. Connect one end of the RS-232 modem cable to the port.
2. Connect the other cable end to a 9-pin serial communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
3. Power on the maintenance terminal. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu appears.

NOTE: The following steps describe changing network addresses using HyperTerminal serial communication software.

4. Open the *HyperTerminal* window on your *Windows Workstation* (*Start>Programs>Accessories>Communications>HyperTerminal*). The *Connection Description* dialog box appears (Figure 2-15).

Figure 2-15 Connection Description Dialog Box

5. Type a descriptive product name in the *Name* field and click *OK*. The *Connect To* dialog box appears.
6. Ensure that the *Connect using* field displays **COM1** or **COM2** (depending on the port connection to the product), and click *OK*. The *COMn Properties* dialog box appears, where *n* is **1** or **2**.

7. Configure *Port Settings* parameters:
   - *Bits per second* - **115200**.
   - *Data bits* - **8**.
   - *Parity* - **None**.
   - *Stop bits* - **1**.
   - *Flow control* - **Hardware** or **None**.

   Click *OK*. The *New Connection - HyperTerminal* window appears.
8. Type the user password (default is **password**) at the **>** prompt, and press **Enter**. The password is case sensitive. The *New Connection - HyperTerminal* window appears with software and hardware version information for the product, and a **C >** prompt at the bottom of the window.
9. Type the **ipconfig** command at the **C >** prompt, and press **Enter**. The *New Connection - HyperTerminal* window appears with configuration information listed:
   - *MAC Address*.
   - *IP Address* (default is **10.1.1.10**).
   - *Subnet Mask* (default is **255.0.0.0**).
   - *Gateway Address* (default is **0.0.0.0**).
   - *Auto Negotiate*.
   - *Speed*.
   - *Duplex*.

   Only the *IP Address*, *Subnet Mask*, and *Gateway Address* fields are configurable.
10. Change the IP address, subnet mask, and gateway address as directed by the customer. To change the addresses, type the following at the **C >** prompt and press **Enter**.

    ipconfig ***xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy*** *zzz.zzz.zzz.zzz*

    The IP address is ***xxx.xxx.xxx.xxx***, the subnet mask is ***yyy.yyy.yyy.yyy***, and the gateway address is *zzz.zzz.zzz.zzz*, where the octets ***xxx***, ***yyy***, and *zzz* are decimals from zero through 255. If an address is to remain unchanged, type the current address in the respective field.

11. Select *Exit* from the *File* pull-down menu. A HyperTerminal message box appears.
12. Click *Yes*. A second message box appears.
13. Click *No* to exit and close the application.
14. Power off the maintenance terminal and disconnect the RS-232 modem cable. Replace the protective cap over the maintenance port.
15. At the product front panel, press and hold the **RESET** button for ten seconds to perform a POR.
16. Connect the product to the customer-supplied Ethernet LAN segment or Ethernet hub:
    a. Connect one end of the Ethernet patch cable (supplied) to the RJ-45 connector (labelled **10/100**).
    b. Connect the remaining end of the cable to the LAN as directed by the customer or to any available Ethernet hub port.
17. Perform one of the following:
    — If the product is delivered separately from the management server, go to *Task 6: Unpack, Inspect, and Install the Management Server*.
    — If the product is delivered as part of a Fabricenter equipment cabinet, go to *Task 7: Configure Server Password and Network Addresses*.

Task 6: Unpack, Inspect, and Install the Management Server

The management server is rack-mount unit with SAN management and Element Manager applications installed. The server also includes a TightVNC Viewer client-server software control package that provides remote network access (through a standard web browser) to the server desktop. For information, refer to www.tightvnc.com.

NOTE: The server and related applications provide a GUI to monitor and manage products, and are a dedicated solution that should not be used for other tasks. Applications on the server are tested, but not compatibility tested with other third-party software. Modifications to the server hardware or installation of additional software (including patches or service packs) may interfere with normal operation.

To unpack, inspect, and install the server use the following steps:

1. Inspect shipping container(s) for damage. Ensure that a freight carrier representative is present when the container is opened. Unpack shipping container(s) and inspect each item for damage. Ensure that the packaged items correspond to items listed on the enclosed bill of materials.
2. Call the toll-free telephone number printed on the attached service label if any items are damaged or missing,
3. Perform one of the following:
   - Desktop installation: Position the server on a table or desktop as directed by the customer. Ensure a grounded AC electrical outlet is available.
   - Cabinet installation: Open the rack-mount kit and inspect the contents. Refer to the enclosed bill of materials and verify all parts are delivered. Install the management server in the equipment cabinet. Refer to the *1U Server Rack-Mount Kit Installation Instructions* (958-000310) for instructions.
4. Connect the server to the customer-supplied Ethernet LAN segment or Ethernet hub (private LAN interface):
   a. Connect one end of the Ethernet patch cable (supplied) as shown in Figure 2-16, to the right RJ-45 adapter (**LAN 2**) at the rear of the server.

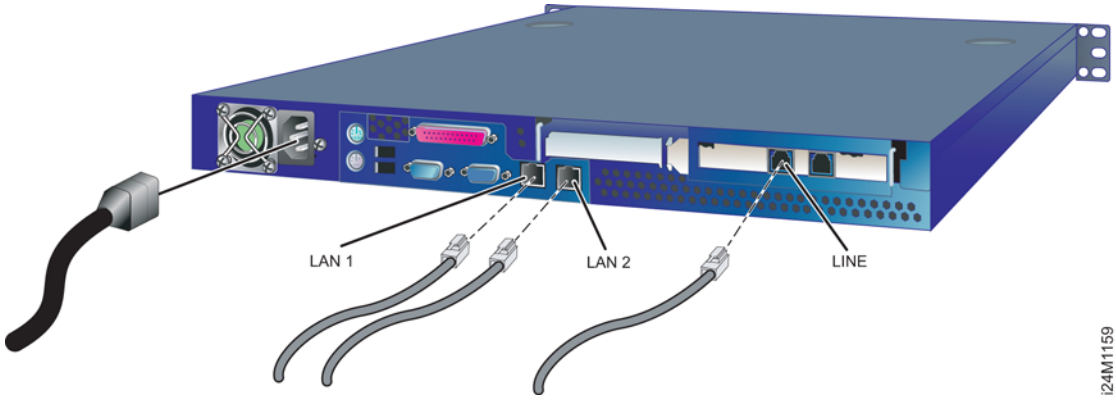


Figure 2-16 1U Management Server Connections

b. Connect the remaining end of the Ethernet cable to the LAN:

- If the server is installed on a customer-supplied LAN segment, connect the cable to the LAN as directed.
- If the server is installed through the Ethernet hub, connect the cable to any available hub port.

5. If required, connect the server to the customer intranet (public LAN interface):

   a. Connect one end of a customer- supplied Ethernet patch cable as shown in Figure 2-16, to the left RJ-45 adapter (**LAN 1**) at the rear of the server.

   b. Connect the remaining end of the Ethernet cable to the corporate intranet as directed by the customer.

6. Connect a phone cord to the left RJ-11 adapter (**LINE**), as shown in Figure 2-16, at the rear of the server and a facility telephone connection.

7. Connect the AC power cord to the server and a facility power source or rack power strip, as shown in Figure 2-16, that provides single-phase, 90 to 264 VAC current.

8. When the power cord is connected, the server powers on and performs power-on self-tests (POSTs). During POSTs:

   a. The green liquid crystal display (LCD) panel illuminates.

   b. The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.

   c. After a few seconds, LCD panel displays a **Boot from LAN? Press <Enter>** message.

   d. Ignore the message. After ten seconds, the server performs the boot sequence from the basic input/output system (BIOS). After successful boot and POST completion, the LCD panel displays a **Welcome!!** message.

   e. The server then continuously cycles through and displays operational information at the LCD panel.

9. Press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive. Insert a blank rewritable CD into the CD-RW drive and close the panel.

Task 7: Configure Server Password and Network Addresses

Verify the LAN installation. If the server or Fabricenter equipment cabinet is installed on a dedicated LAN, network information does not require change. Change the default password for the server LCD panel (if required by the customer), then go to *Task 8: Configure Management Server Information*.

If the server or equipment cabinet is installed on a public LAN, the default password for the server LCD panel and the following transmission control protocol internet protocol (TCP/IP) network information must be changed to conform to the customer's LAN addressing scheme:

- IP address.
- Subnet mask.

Configure Password

To configure a new LCD panel password:

1. Press **ENTER** at the management server LCD panel . The **Welcome!!** or operational information message changes to an **Input Password 0****** message.
2. Using the ▲ button to increment a digit, the ▼ button to decrement a digit, the ◄ button to move the cursor left, and the ► button to move the cursor right, input the default password (**9999**), and press **ENTER**. A **LAN 1 Setting??** message appears at the LCD panel.
3. Press the ▼ button several times until the **Change Password?** option appears at the LCD panel, then press **ENTER**. A **New Password 0****** message appears.
4. Use the arrow keys as described in step 2 to input a new 4-digit numeric password, then press **ENTER**. A **Save Change? Yes, Save!!** message appears.
5. Press **ENTER**. A **Wait a moment!** message appears at the LCD panel, the LCD panel returns to the **LAN 1 Setting??** message, and the password changes.

Configure Private LAN Addresses

To configure TCP/IP network information for the private LAN connection (LAN 2):

1. Press **ENTER,** at the management server LCD panel, press **ENTER**. The **Welcome!!** or operational information message changes to an **Input Password 0****** message.
2. Using the ▲ button to increment a digit, the ▼ button to decrement a digit, the ◄ button to move the cursor left, and the ► button to move the cursor right, input the default or changed password, and press **ENTER**. The **LAN 1 Setting??** message appears at the LCD panel.
3. Press the ▼ button. The **LAN 2 Setting??** message appears at the LCD panel. Press **ENTER** and the default IP address of **10.1.1.1** appears.
4. Use the arrow keys as described in step 2 to input a new IP address, then press **ENTER**. A **Save Change? Yes, Save!!** message appears.
5. Press **ENTER**. The LAN 2 IP address changes and the default subnet mask of **255.0.0.0** appears.
6. Use the arrow keys as described in step 2 to input a new subnet mask, then press **ENTER**. A **Save Change? Yes, Save!!** message appears.
7. Press **ENTER**. A **Wait a moment!** message appears at the LCD panel, the panel returns to the **LAN 1 Setting??** message, and the LAN 2 subnet mask changes.
8. Record the private LAN IP address and subnet mask for reference if the server hard drive fails and must be restored.

Configure Public LAN Addresses (Optional)

To optionally configure TCP/IP network information for the public LAN connection (LAN 1):

1. Press **ENTER** at the management server LCD panel, . The **Welcome!!** or operational information message changes to an **Input Password 0****** message.
2. Using the ▲ button to increment a digit, the ▼ button to decrement a digit, the ◄ button to move the cursor left, and the ► button to move the cursor right, input the default or changed password, and press **ENTER**. The **LAN 1 Setting??** message appears at the LCD panel.

3. Press **ENTER** and the default IP address of **192.168.0.1**. appears.
4. Use the arrow keys as described in step 2 to input a new IP address, then press **ENTER**. A **Save Change? Yes, Save!!** message appears.
5. Press **ENTER**. The LAN 1 IP address changes and the default subnet mask of **255.0.0.0** appears.
6. Use the arrow keys as described in step 2 to input a new subnet mask, then press **ENTER**. A **Save Change? Yes, Save!!** message appears.
7. Press **ENTER**. A **Wait a moment!** message appears at the LCD panel, the panel returns to the **LAN 1 Setting??** message, and the LAN 1 subnet mask changes.
8. Record the public LAN IP address and subnet mask for reference if the server hard drive fails and must be restored.

Task 8: Configure Management Server Information

Configure a server computer name and workgroup name from the Windows operating system, using a LAN-attached PC with standard web browser.

If required, change the server's gateway addresses and domain name system (DNS) server IP addresses to conform to the customer's LAN addressing scheme. The gateway addresses are the addresses of the local router for the corporate intranet.

Access the Management Server Desktop

To login and access the server desktop use the following steps:

1. Ensure that the management server and a browser-capable PC are connected through an Ethernet LAN. Launch the browser application (Netscape Navigator or Internet Explorer).
2. Enter the **LAN 2** IP address of the server, followed by **:5800**, as the Internet uniform resource locator (URL). Use the following format:

   http://xxx.xxx.xxx.xxx:5800

Where ***xxx.xxx.xxx.xxx*** is the default IP address of **10.1.1.1** or the IP address configured while performing *Task 7: Configure Server Password and Network Addresses*. The *VNC Authentication* screen appears.

3. Type the default password and click *OK*. The *Welcome to Windows* dialog box appears.

NOTE: The default TightVNC viewer password is **password.**

4. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the server desktop. The *Log On to Windows* dialog box appears.

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the server.

5. Type the default Windows user name and password and click *OK*. The server's Windows desktop opens and the *EFCM Log In* dialog box appears.

NOTE: The default Windows user name is **Administrator** and the default password is **password**. Both are case-sensitive.

Configure Management Server Names

To configure the management server name and workgroup name use the following steps:

1. Open the system properties dialog box from the Windows desktop (*Start>Settings>Control Panel>System*). The *System Properties* dialog box appears with the *General* tab open by default.
2. Click the *Network Identification* tab. The *System Properties* dialog box appears with the *Network Identification* tab selected.
3. Click *Properties*. The *Identification Changes* dialog box appears (Figure 2-17).

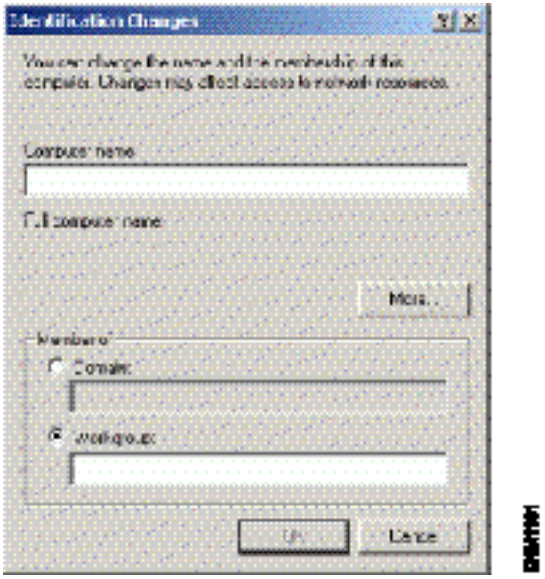


Figure 2-17 Identification Changes Dialog Box

4. Change the name to **MGMTSERVER** at the *Computer Name* field. Click (select) the *Workgroup* radio button, change the name to **WORKGROUP**, and click *OK*. The dialog box closes.
5. Record the computer and workgroup names for reference if the server hard drive fails and must be restored.
6. Close all dialog boxes and return to the Windows desktop.

Configure Gateway and DNS Server Addresses

To configure gateway and DNS server IP addresses for the private LAN connection (**LAN 2**) and public LAN connection (**LAN 1**):

1. Open the system properties dialog box from the Windows desktop (Start>Settings>Control Panel>Network and Dial-up Connections). The *Network and Dial-up Connections* window appears.
2. To configure addresses for the private LAN connection (**LAN 2**), double-click the *Local Area Connection 2* icon. The *Local Area Connection 2 Status* dialog box appears.
3. Click *Properties*. The *Local Area Connection 2 Properties* dialog box appears.

4. In the *Components checked are used by this connection* field, double-click the *Internet Protocol (TCP/IP)* entry. The *Internet Protocol (TCP/IP) Properties* dialog box appears (Figure 2-18).

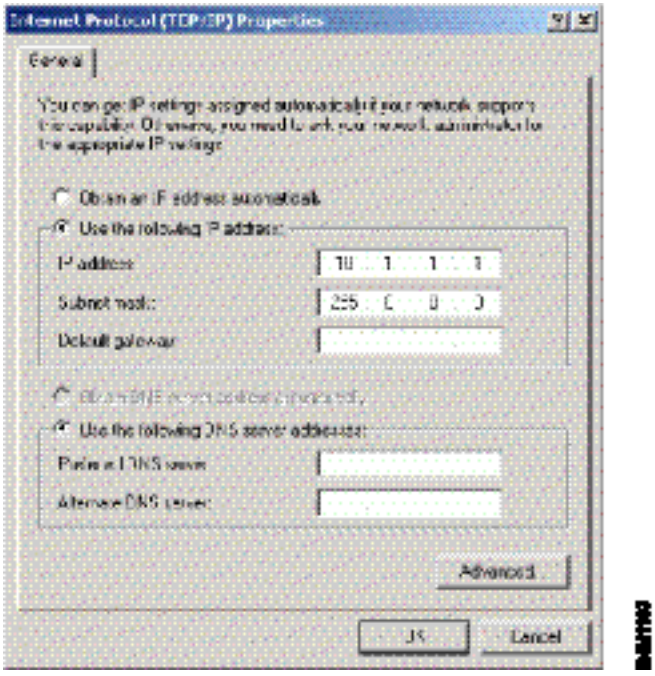


Figure 2-18 Internet Protocol (TCP/IP) Properties Dialog Box

5. The *Use the following IP address* radio button is enabled and the *IP address* and *Subnet mask* fields display network information configured while performing *Task 7: Configure Server Password and Network Addresses*.
6. Enter the gateway address obtained from the customer at the *Default gateway* field.
7. Select (enable) the *Use the following DNS server addresses* radio button. At the *Preferred DNS server* field, enter the DNS server IP address obtained from the customer, then click *OK* to apply the changes and close the dialog box.

8. Close dialog boxes as appropriate and return to the The *Network and Dial-up Connections* window.
9. Record the changed gateway and DNS server addresses for reference if the server hard drive fails and must be restored.
10. To optionally configure addresses for the public LAN connection (**LAN 1**), double-click the *Local Area Connection 1* icon and repeat step 2 through step 9.
11. Close all dialog boxes and return to the Windows desktop.
12. Reboot the server and *Access the Management Server Desktop*.

Task 9: Configure Windows Operating System Users

Configure password access for all authorized Windows (server) users. It is also recommended to change the default administrator password. To configure users:

1. Open the system properties dialog box from the Windows desktop (Start>Settings>Control Panel>*Users and Passwords*). The *Users and Passwords* dialog box appears.
2. The *Guest* user name is a built-in account in the Windows operating system and cannot be deleted. The *srvacc* account is for field service users and must not be modified or deleted.

Change Default Administrator Password

To change the administrator password from the default (**password**) to a customer-specified password:

1. Click *Set Password* at the *Users and Passwords* dialog box. The *Set Password* dialog box appears.
2. *Confirm New Password* fields at the *New Password* and, type the new password. Both fields are case-sensitive.
3. Click *OK*. The default administrator password changes and the *Set Password* dialog box closes.

Add a New User

To set up a new Windows user:

1. Click *Add* at the *Users and Passwords* dialog box, . The first window of the *Add New User* wizard appears (Figure 2-19).

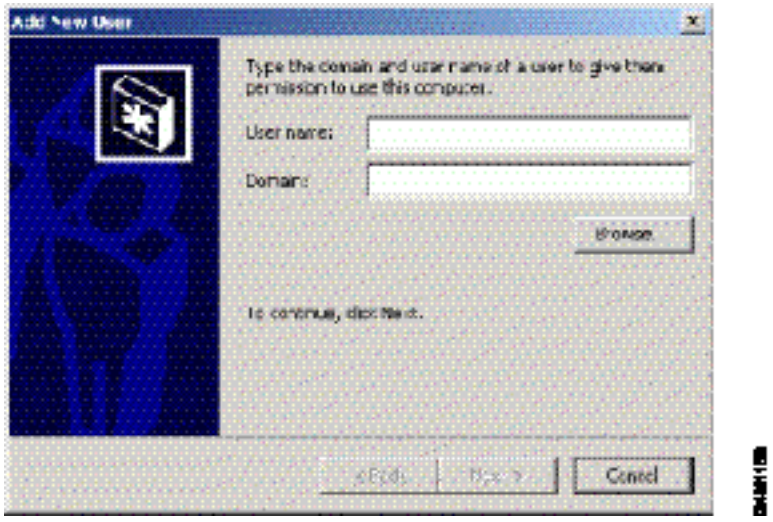

Add New User
Type the domain and user name of a user to give them permission to use this computer.
User name:
Domain:
Browse...
To continue, click Next.
< Back
Next >
Cancel

Figure 2-19 Add New User Wizard

2. Type the appropriate information in the *User name* and *Domain* fields and click *Next*. The second window of the *Add New User* wizard appears.
3. Type the new user password in the *Password* and *Confirm password* fields and click *Next*. The third window of the *Add New User* wizard appears.
4. Based on the level of access to be granted, select the *Standard user*, *Restricted user*, or *Other* radio button. If the *Other* radio button is selected, choose the type of access from the adjacent list box.
5. Click *Finish*. New user information is added and the wizard closes. Record the user information for reference if the server hard drive fails and must be restored.
6. If no other users are to be added, close all dialog boxes and return to the Windows desktop.

Change User Properties

To change existing user properties use the following steps:

1. Highlight the user at the *Users for this computer* field and click *Properties* at the *Users and Passwords* dialog box. The *Properties* dialog box appears with the *General* tab selected (Figure 2-20).

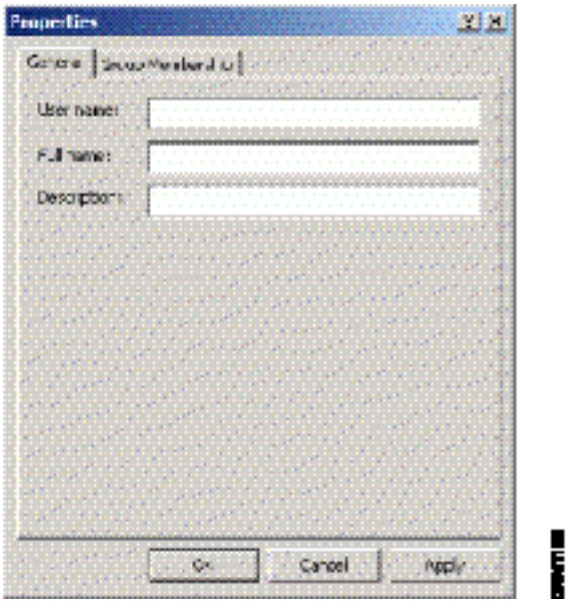


Figure 2-20 Properties Dialog Box (General Tab)

2. Type the appropriate new user information in the *User name*, *Full name*, and *Description* fields, then click the *Group Membership* tab. The *Properties* dialog box appears with the *Group Membership* tab selected.
3. Select the *Standard user*, *Restricted user*, or *Other* radio button based on the level of access to be changed, . If the *Other* radio button is selected, choose the type of access from the adjacent list box.
4. Click *OK*. The new user information is added and the *Properties* dialog box closes. Record the user information for reference if the server hard drive fails and must be restored.
5. Close all dialog boxes and return to the Windows desktop.

Task 10: Set Management Server Date and Time

SAN Management application logs are stamped with the server date and time, and the product system clock is synchronized with the server date and time by default. To set the server date and time:

1. Open the system properties dialog box from the Windows desktop (Start>Settings>Control Panel>*Date/Time*). The *Date/Time Properties* dialog box appears with the *Date & Time* page open.

   NOTE: The *Time Zone* field must be set before the *Date & Time* field.

2. Click the *Time Zone* tab. The *Date/Time Properties* dialog box appears with the *Time Zone* page open (Figure 2-21).

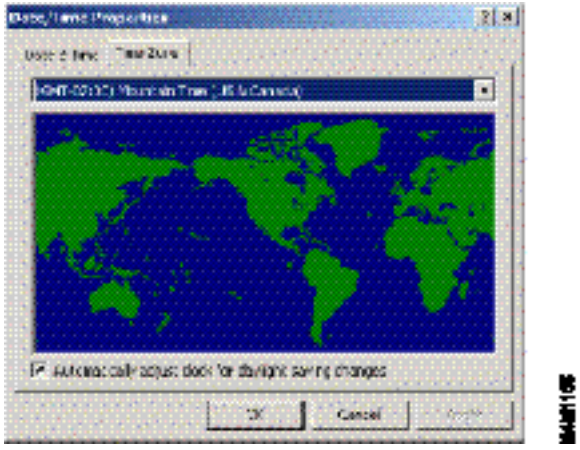


Figure 2-21 Date/Time Properties Dialog Box (Time Zone Tab)

3. To change the time zone use the following steps:
   a. Select the appropriate time zone from the drop-down list at the top of the dialog box.
   b. If instructed by the customer, select the *Automatically adjust clock for daylight saving changes* check box.
   c. Click *Apply*. Record time zone and daylight savings information for reference if the server hard drive fails and must be restored.
4. Click the *Date & Time* tab. The *Date/Time Properties* dialog box appears with the *Date & Time* page open (Figure 2-22).

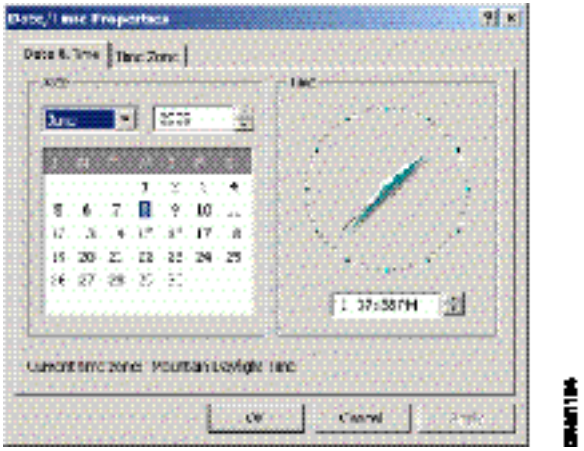


Figure 2-22 Date/Time Properties Dialog Box (Date & Time Tab)

5. To change the date and time use the following steps:
   a. Select the month from the drop-down list under *Date*.
   b. Click the up or down arrow adjacent to the year field and select the desired year.
   c. Click the day on the calendar to select the desired date.
   d. Click in the time field and enter the desired time, then click the adjacent up or down arrow and select *AM* or *PM*.
   e. Click *Apply*. Record date and time information for reference if the server hard drive fails and must be restored.
6. Close all dialog boxes and return to the Windows desktop.

Task 11: Configure the Call-Home Feature (Optional)

The management server has an optional call-home feature that provides automatic dial-out through the internal modem to a service support facility to report switch problems. The problem is logged into the support facility's tracking system for resolution. To configure the call-home feature:

1. There are two jacks on the server internal modem: one for the call-home connection (**LINE**), and the other for a telephone (**PHONE**). Ensure a telephone cable is routed and connected to the **LINE** jack at the rear of the management server (connected while performing *Task 6: Unpack, Inspect, and Install the Management Server*).
2. Double-click the *Call Home Configuration* icon at the Windows desktop. The *Call Home Configuration* dialog box appears.
3. Enter the telephone number for the technical support center (**800-752-4572**) at the *Call Center Phone Number* field. Include necessary information, such as the country code, area code, or any prefix required to access a telephone line outside the facility.
4. Enter the telephone number for access to the local server at the *Local Phone Number* field. Include necessary information such as the country code or area code.
5. Click *OK* to save the configured telephone numbers and close the dialog box.

Task 12: Assign User Names and Passwords

In addition to password access for the Windows operating system, users must be configured for SAN management application access. To assign application user names and passwords use the following steps:

1. The *EFCM Log In* dialog box appears at the Windows desktop. The dialog box was opened when performing *Task 8: Configure Management Server Information*.
2. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

   NOTE: The default user ID is **Administrator** and the default password is **password.** Both are case-sensitive.

3. Click *Login*. The application opens and the EFCM main window appears.
4. Select *Users* from the *SAN* menu. The *EFCM Server Users* dialog box appears.

5. Click *Add*. The *Add User* dialog box appears (Figure 2-23).

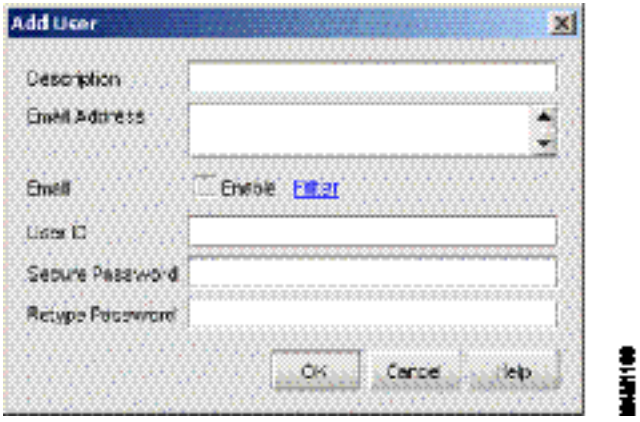


Figure 2-23 Add User Dialog Box

6. Enter information in fields as directed by the customer:
   - **Description -** Type a new user name up to 16 alphanumeric characters in length. Control characters and spaces are not valid. The user name is case-sensitive.
   - **Email Address -** Type one or more new user e-mail addresses. Separate multiple addresses with a semicolon.
   - **User ID -** Type a unique user ID for the new user.
   - **Secure password -** Type a password up to 16 alphanumeric characters in length. Control characters and spaces are not valid. The password is case-sensitive.
   - **Retype Password -** To confirm the password, enter the password exactly as in the *Secure Password* field.
7. Enable the *Enable* check box to enable e-mail notification for the new user. An unchecked box indicates e-mail notification is not enabled.
8. Select (click) the *Filter* link to configure event types for which e-mail notification is sent. The *Define Filter* dialog box appears. For instructions on defining event filters, refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170).
9. Click *OK* to accept the information. Close all dialog boxes and return to the EFCM main window.

Task 13: Configure the Product to the Management Application

To manage a new product, it must be identified to and discovered by the SAN management application. To identify the product use the following steps:

1. Select *Setup* from the *Discover* menu (*Discover>Setup*). The *Discover Setup* dialog box appears.
2. Click *Add*. The *Address Properties* dialog box appears with the *IP Address* page open by default (Figure 2-24).

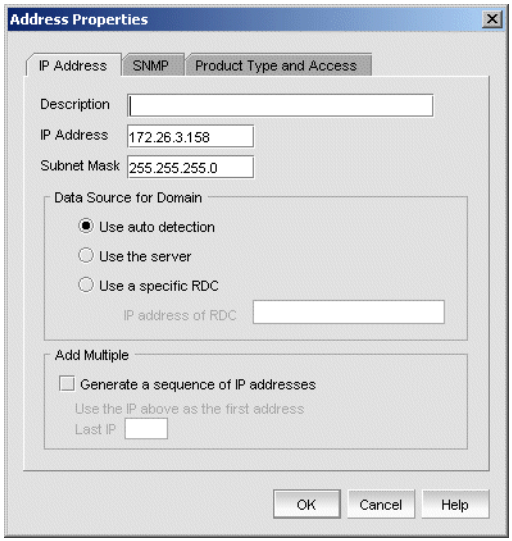


Figure 2-24 Address Properties Dialog Box (IP Address Page)

3. Type a product description in the *Description* field.
4. Type the product IP address (determined by the customer) in the *IP Address* field.
5. Type the product subnet mask (determined by the customer) in the *Subnet Mask* field.
6. Click *OK* to save the entered information and define the switch to the SAN management application. Close all dialog boxes and return to the EFCM main window.

Task 14: Record or Verify Server Restore Information

Windows operating system configuration information must be recorded to restore the server in case of hard drive failure. Refer to Appendix B, *Restore Management Server* for instructions. Record or verify the following information:

1. Ensure that the network configuration information was recorded while performing *Task 7: Configure Server Password and Network Addresses* and *Task 8: Configure Management Server Information*.
   a. The default LCD panel password (**9999**) or changed password was recorded.
   b. The default or changed network addresses were recorded for the private LAN connection **(LAN 2**):
      - **IP address -** default is **10.1.1.1**.
      - **Subnet mask -** default is **255.0.0.0**.
      - **Gateway address -** default is blank.
      - **DNS server IP address -** default is blank.
   c. The default or changed network addresses were recorded for the public LAN connection (**LAN 1**):
      - **IP address -** default is **192.168.0.1**.
      - **Subnet mask -** default is **255.0.0.0**.
      - **Gateway address -** default is blank.
      - **DNS server IP address -** default is blank.
   d. The default computer name (**MGMTSERVER**) or changed computer name was recorded.
2. Ensure that the user passwords and other information were recorded while performing *Task 9: Configure Windows Operating System Users*.
3. Ensure the date and time information was recorded while performing *Task 10: Set Management Server Date and Time*.
   a. Ensure that the time zone was recorded.
   b. Ensure if the management server was set to automatically adjust the clock for daylight savings time changes.
4. Record the Product ID number:

a. Open the system properties dialog box from the Windows desktop (Start>Settings>Control Panel.>System). The *System Properties* dialog box appears with the *General* tab open by default.

b. Record the Product ID number listed under the *Registered to* heading.

c. Close all dialog boxes and return to the Windows desktop.

Task 15: Verify Product-to-Server Communication

Communication must be verified between the product and server (SAN management and Element Manager applications). To verify communication use the following steps:

1. At the SAN management application main window (physical map or product list), inspect the shape and color of the status symbol associated with the product icon. Table 2-4 explains operational states and associated symbols.

Table 2-4 Operational States and Symbols

Operational State	Status Symbol
Operational - Communication is established, the product is operational, and no failures are indicated. Go to *Task 16: Configure PFE Key (Optional)*.	No status symbol
Degraded - Communication is established, but the product is operating in degraded mode and requires service. This condition is typical if a port or redundant FRU fails. Go to step 2.	
Failed - Communication is established, but the product failed and requires immediate service. Go to step 2.	
Status Unknown - Product status is unknown because of a network communication failure. Go to step 2.	

2. Right-click the product icon at the SAN management application's physical map. A pop-up menu appears.

3. Select the *Element Manager* option from the pop-up menu. When the Element Manager application opens, the last view accessed by a user opens by default. As an example, the *Hardware View* (Figure 2-25) is shown.

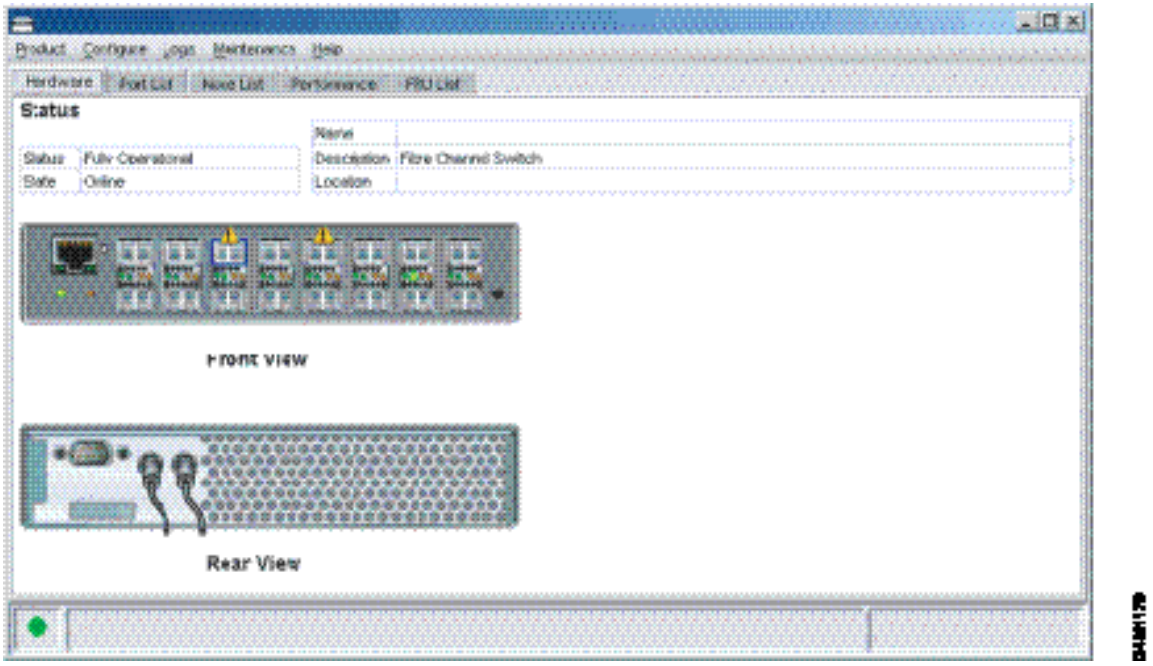


Figure 2-25 Hardware View

4. Inspect product status at the *Hardware* view and perform one of the following steps:
   - If the product appears operational (no FRU alert symbols and a green circle at the status bar), go to *Task 16: Configure PFE Key (Optional)*.
   - If product operation appears degraded or a failure is indicated (FRU alert symbols and a yellow triangle or red diamond on the status bar), go to *MAP 0000: Start MAP* to isolate the problem.

Task 16: Configure PFE Key (Optional)

Follow the procedures in this section to install optional features using PFE key.

After purchasing a feature, obtain the PFE key by following the enclosed instructions. The key is an alphanumeric string consisting of uppercase and lowercase characters that must be entered exactly, including dashes.

Keys are encoded to work only with the serial number of the installed product. Note down the key. This will help you to re-install the feature when required.

If the product fails and is replaced, obtain new PFE keys from the technical support center (**800-752-4572** or **support@mcdata.com**).

You will have to provide the serial numbers of the failed and replacement products and the old PFE key number or transaction code.

The optional features that you can install using PFE keys are listed below:

- **Element Manager application -** This feature enables out-of-band product management through an Element Manager interface. Products are delivered with the application enabled for a 31-day grace period. Before grace period expiration, the application must be reactivated through a PFE key.

  During the grace period, a *No Feature Key* dialog box appears when the Element Manager application opens. Click *OK* to close the dialog box and use the application. In addition, the message **Element Manager license key has not been installed - Please follow up instructions to update permanent key** appears splashed across all views.

- **Flexport Technology -** A Flexport Technology product is delivered at a discount without all Fibre Channel ports enabled. When additional port capacity is required, the remaining ports are incrementally enabled through this feature.

- **Full volatility -** This feature ensures no Fibre Channel frames are stored after the product is powered off or fails, and a memory dump file (that possibly includes classified data frames) is not included as part of the data collection procedure.

- **N_Port ID virtualization -** This feature allows up to 256 Fibre Channel addresses to be assigned to an N_Port.
- **OpenTrunking -** This feature provides dynamic load balancing of Fibre Channel traffic across multiple ISLs.
- **SANtegrity (enhanced) -** This feature enhances security in SANs by combining the functions of SANtegrity authentication (restricting access to Fibre Channel elements) and SANtegrity binding (controlling large and mixed fabrics).

After obtaining a PFE key, install the feature as follows:

1. Select *Features* from the *Configure* menu at any view. The *Configure Feature Key* dialog box appears.
2. Click *New*. The *New Feature Key* dialog box appears (Figure 2-26).

Figure 2-26 New Feature Key Dialog Box

3. Type the PFE key (case-sensitive **xxxx-xxxx-xxxx-xx** format) and click *OK*. The *Enable Feature Key* dialog box appears.
4. Ensure that the feature description appears in the *New Features* panel and click *OK*. A *Warning* dialog box appears with the message **Installing this feature key causes an IPL and momentary loss of the LAN connection. The operation is nondisruptive to Fibre Channel traffic. Do you wish to continue?**
5. Click *Yes* to enable the PFE key and IPL the product. Close all dialog boxes and return to the Element Manager application.

Task 17: Configure Management Server (Optional)

Folllow the procedures in this section to configure the open systems management server and enable OSI host control of the product.

NOTE: Implementing host control requires installation of a SAN management application on the OSI server. Management applications include Veritas® SANPoint™ Control or Tivoli® NetView®.

To configure the management server, use the following steps:

1. Select *Open Systems Management Server* from the *Configure* menu at any view. Two submenu options display:
   - *Enable OSMS*.
   - *Host Control Prohibited*.
2. Enable or disable OSMS by selecting the *Enable OSMS* option. Check the box to enable the server.
3. Allow or prohibit host (OSI server) control by selecting the *Host Control Prohibited* option. Check the box to prohibit a host management program from changing configuration and connectivity parameters on the product. The host program has read-only access to configuration and connectivity parameters.

Task 18: Set Product Date and Time

Log entries are stamped with the date and time received from the product. To set the effective date and time for the product:

1. Select *Date/Time* from the *Configure* menu (*Configure>Date/Time*). The *Configure Date and Time* dialog box appears (Figure 2-27).

   Date and time can be set manually, or set to be periodically updated by the SAN management application (the product and application synchronize at least once daily).

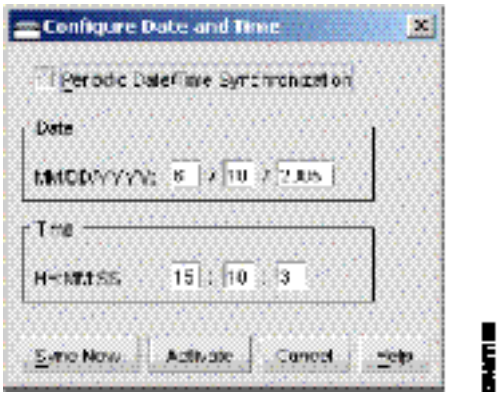


Figure 2-27 Configure Date and Time Dialog Box

2. To set date and time manually:
   a. Disable (uncheck) the *Periodic Date/Time Synchronization* check box. The *Date* and *Time* fields become active.
   b. Configure the *Date* field:
      - Month (*MM*): **1** through **12**.
      - Day (*DD*): **1** through **31**.
      - Year (*YYYY*): greater than **1980**.
   c. Configure the *Time* field:
      - Hour (*HH*): **0** through **23**.
      - Minute (*MM*): **0** through **59**.
      - Second (*SS*): **0** through **59**.
   d. Click *Activate* to set the switch date and time and close the dialog box.
3. Use the following procedure to set the product to periodically synchronize date and time with the SAN management application:
   a. Click the *Periodic Date/Time Synchronization* check box to select the option.
   b. Do one of the following:

- Click *Activate* to enable synchronization and close the dialog box. Product date and time synchronize with the SAN management application date and time at the next update period (at least once daily).
- Click *Sync Now* to synchronize the product and SAN management application immediately. The *Date and Time Synced* information dialog box appears. Click *OK* to synchronize the date and time and close the dialog box, then click *Activate* to enable synchronization and close the *Configure Date and Time* dialog box.

Task 19: Configure the Element Manager Application

To configure the Element Manager application, selectively perform the following tasks according to customer requirements:

Product	• Identification • Product parameters • Fabric parameters.
Ports	• Basic information • Buffer-to-buffer credits (BB_Credits) • N_Port identifier virtualization (NPIV).
Management	• SNMP trap message recipients • Threshold alerts • EFCM Basic Edition interface access • Telnet access • e-mail, Ethernet event, and call-home event notification.
Security	• SANtegrity authentication • Enterprise Fabric Mode • SANtegrity binding.
Interswitch links	• OpenTrunking • Preferred path • ISL port fencing

Configure Product Identification

Follow the procedures in this section to configure the product identification.

NOTE: The *Name*, *Location*, and *Contact* variables correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*, and are used by management workstations when obtaining product data.

1. Select *Operating Parameters* from the *Configure* menu (*Configure*>*Operating Parameters*). The *Operating Parameters* dialog box appears.
2. Click the Identification tab.(Figure 2-28).

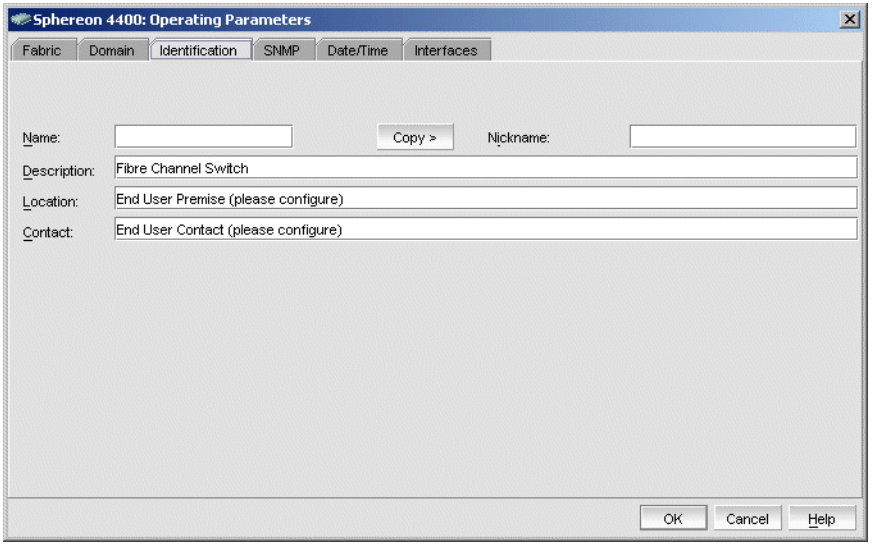


Figure 2-28 Identification View

c. Type a unique product name of 24 alphanumeric characters or less in the Name field. If installed on a public LAN, the name should reflect the product's Ethernet network domain name system (DNS) host name.

d. Type a product description of 255 alphanumeric characters or less in the Description field.

e. Type the product's physical location (255 alphanumeric characters or less) in the Location field.

f. Type the name of a contact person (255 alphanumeric characters or less) in the Contact field.

3. Click *Activate* to save the information and close the dialog box.

Configure Product Parameters

Follow the procedures in this section to configure product operating parameters.

1. Set the product offline. Refer to *Setting Online State* for instructions.
2. Select *Operating Parameters* from the *Configure* menu (*Configure>Operating Parameters*).
3. Click the *Domain* tab (Figure 2-29).

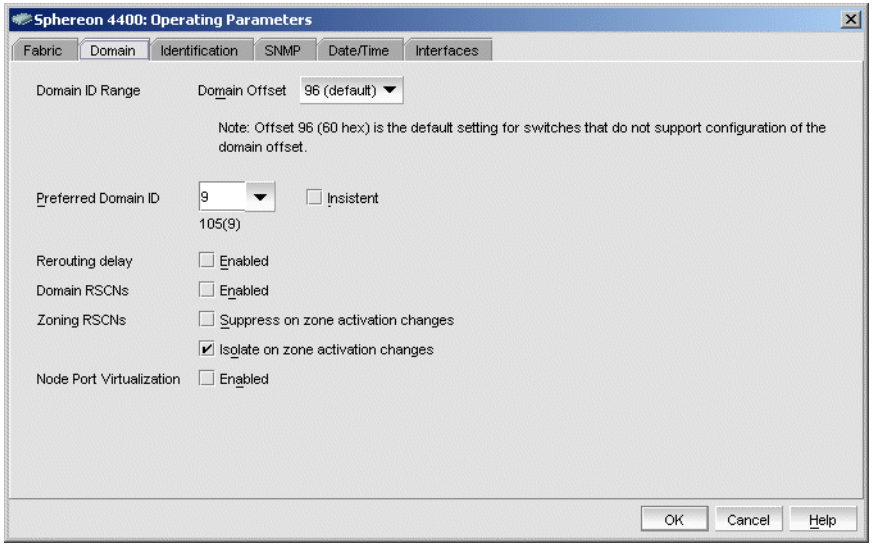


Figure 2-29 Configure Switch Parameters Dialog Box

a. Select the *Domain ID Offset* value from the drop-down list. Values available in the drop-down list are 0, 32, 64, 96 (default), 128, 160, and 192. Domain IDs minus the offset are still in the 1-31 range.

b. Type a value between **1** - **31** in the *Preferred Domain ID* field. This value uniquely identifies each fabric element. At the Preferred Domain ID field, type a value between 1 through 31. This value uniquely identifies each fabric element.

NOTE: An ISL between fabric elements with identical domain IDs segments and prevents communication.

If the *Insistent Domain ID* field is enabled, the value configured in the *Preferred Domain ID* field becomes the active domain ID when the fabric initializes.

c. Enable (check) the *Rerouting Delay* field if you want the traffic to be delayed through the fabric by the user-specified error detect time out value (E_D_TOV). This delay ensures that Fibre Channel frames are delivered to their destination in order.

d. Enable (check) the *Domain RSCNs* field if you want the attached devices to register to receive notification when other devices change state.

e. Enable (check) the *Suppress Zoning RSCNs on Zone Set Activations* field if you do not want the RSCNs to be transmitted when a zone set is activated.

f. Enable (check) the *Isolate on zone activations* field if you want only devices that require RSCN notification, due to a zoning configuration change, to receive RSCNs. Do not enable this option if *Suppress on zone set activations* is enabled because RSCNs will not be sent to attached devices.

g. Enable (check) the *Node Port Virtualization* field for N_Port identifier virtualization (NPIV). NPIV allows multiple (up to 256) F

4. Click *Activate* to save the information and close the dialog box.
5. Set the product online. Refer to *Setting Online State* for instructions.

Configure Fabric Parameters

Follow the procedures in this section to configure fabric operating parameters.

To configure the fabric operating parameters, use the following steps:

1. Set the product offline. Refer to *Setting Online State* for instructions.
2. Select *Operating Parameters* from the *Configure* menu (*Configure>Operating Parameters*). The *Operating Parameters* dialog box appears.

3. Click the *Fabric* tab (Figure 2-30).

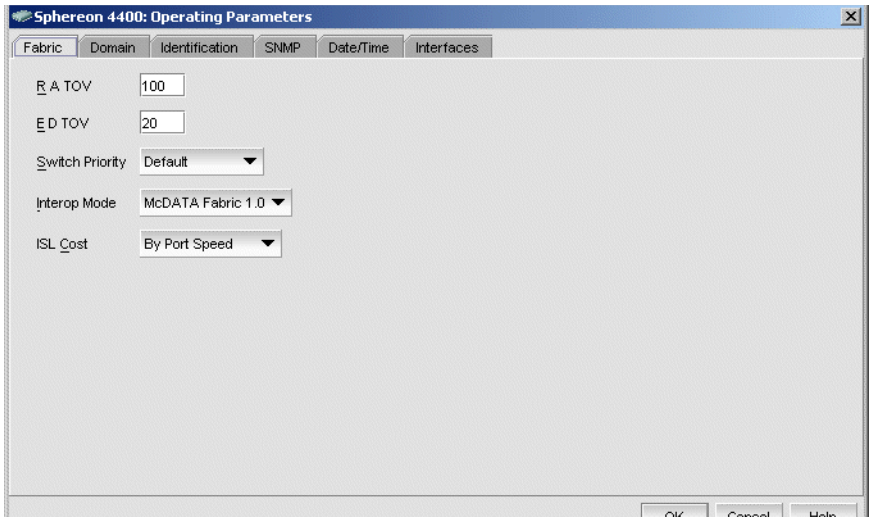


Figure 2-30 Configure Fabric Parameters Dialog Box

a. Type a value between **10** - **1200** tenths of a second (1-120 seconds) in the *R_A_TOV* field. This value must be greater than the E_D_TOV value.

b. Type a value between **2** - **600** tenths of a second (0.2 - 60 seconds) in the *E_D_TOV* field. This must be greater lesser than the R_A_TOV value.

NOTE: Fabric elements must be set to the same R_A_TOV and E_D_TOV values. An ISL between fabric elements with different values segments and prevents communication.

---

c. Select from the *Switch Priority* drop-down list to designate the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself). Available selections are *Default*, *Principal*, and *Never Principal*.

Principal is the highest priority setting, *Default* is next, and *Never Principal* is the lowest. At least one switch in a fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all ISLs segment.

d. Select from the *Interop Mode* drop-down list to set the product operating mode. This setting affects the management mode and does not affect port operation. Available selections are:

- **McDATA Fabric 1.0 -** Select this option if the product is fabric-attached only to other McDATA directors or switches operating in McDATA fabric mode.
- **Open Fabric 1.0 -** Select this option (default) for managing heterogeneous fabrics and if the product is fabric-attached to McDATA directors or switches and other open-fabric compliant switches.

NOTE: With Open Fabric 1.0 enabled, the default zone set is disabled.

e. Select from one of the options to change the ISL cost.

- **By Port Speed** - The fastest fabric path is determined by port (ISL) speed. Cost is inversely proportional to speed.
- **Ignore Port Speed** - ISL speed is ignored, and the fastest fabric path is determined by the number of hops. Cost is directly proportional to hop count.

4. Click *Activate* to save the information and close the dialog box.
5. Set the product online. Refer to *Setting Online State* for instructions.

Configure Ports

Follow the procedure in this section to configure the ports for the product.

To configure Fibre Channel ports, use the following steps:

1. Select *Ports* from the *Configure* menu (*Configure>Ports*). The *Configure Ports* dialog box appears (Figure 2-31).

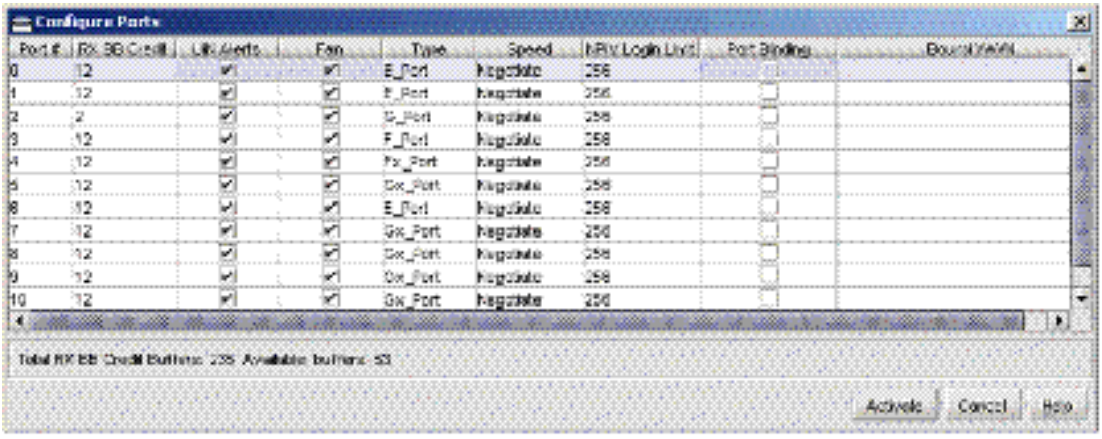


Figure 2-31 Configure Ports Dialog Box

a. Type a port name of 24 alphanumeric characters or less, for each port to be configured, in the *Name* field. The port name should characterize the device to which the port is attached.

b. The switch provides a port buffer pool of 150 receive BB_Credits. Each port can be assigned between two and 120 credits, provided the total credits allocated to all ports does not exceed 150. The default value is six credits per port. Type the desired value in the *RX BB_Credit* column.

c. Enable the check box in the *LIN Alerts* column to enable or disable link incident (LIN) alerts (default is enabled). A check mark indicates alerts are enabled. When enabled and a port incident occurs, an alert indicator (yellow triangle) appears at the *Hardware View* and a message is sent to e-mail recipients.

d. Enable the check box in the *FAN* column to enable or disable the fabric address notification feature (default is enabled). A check mark indicates FAN is enabled. When enabled, an FL_Port transmits FAN frames after loop initialization to verify FC-AL devices are still logged in.

e. Select from the drop-down list in the *Type* column to configure the port type. Available selections are fabric port (**F_Port**), expansion port (**E_Port**), generic port (**G_Port**), generic mixed port (**GX_Port**), and fabric mixed port (**FX_Port**).

f. Select from the drop-down list in the *Speed* column to configure the port transmission rate. Available selections are auto-negotiate between speeds (**Negotiate**), 1.0625 Gbps operation (**1 Gb/sec**), 2.1250 Gbps operation (**2 Gb/sec**), and 4.2500 Gbps operation (**4 Gb/sec**).

g. The NPIV feature must be installed to allow multiple Fibre Channel addresses to be assigned to an N_Port. Refer to *Installing PFE Keys (Optional)* for instructions. Type the desired value (**1** - **256**) in the *NPIV Login Limit* column.

h. Enable the check box in the *Port Binding* column to enable or disable the feature (default is disabled). A check mark indicates binding is enabled and the port can connect only to a device with a WWN listed in the *Bound WWN* column.

i. Type the WWN or nickname of the device attached to the port in the *Bound WWN* column.

- If port binding is enabled and a WWN or nickname appears in the *Bound WWN* column, only the specified device can connect.
- If port binding is enabled but no WWN or nickname appears in the *Bound WWN* column, no device can connect.
- If port binding is disabled, any device can connect.

2. Click *Activate* to save the information and close the dialog box.

Configure SNMP

Follow the procedures in this section to configure names, write authorizations, addresses, and UDP port numbers for SNMP trap message recipients. To configure recipient workstations:

1. Select *Operating Parameters* from the *Configure* menu(Configure>Operating Parameters). The *Operating Parameters* dialog box appears.

1. Select the *SNMP* tab (Figure 2-32).

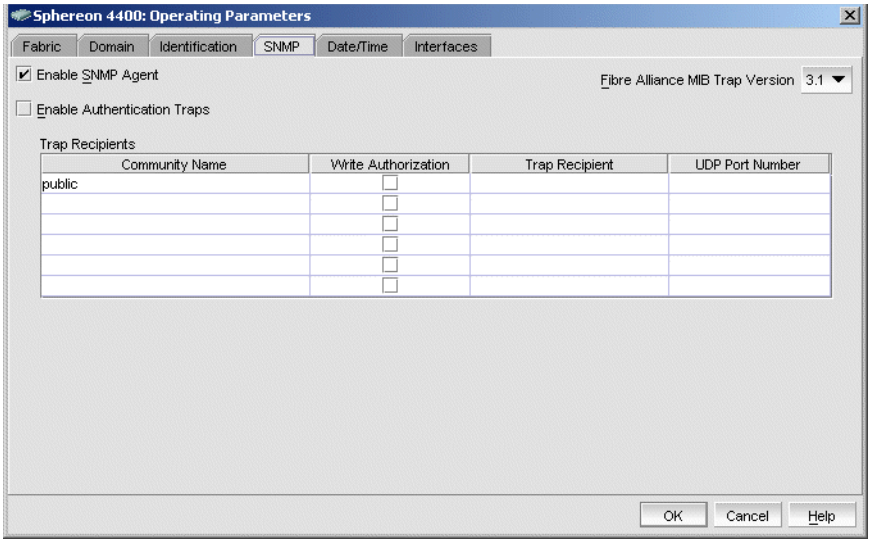


Figure 2-32 Configure SNMP Dialog Box

a. Enable the *Enable SNMP Agent* and *Enable Authentication Traps* to activate the installed agent and enable transmission of SNMP trap messages to recipients.

b. Select the appropriate FA MIB from the *Fibre Alliance MIB Trap Version* drop-down list. Valid selections are **FA MIB Version 3.0** or **FA MIB Version 3.1**.

c. Type a community name of 32 alphanumeric characters or less, for each configured recipient, in the *Community Name* field. The name is incorporated in SNMP trap messages to ensure against unauthorized viewing.

d. Enable the check the box in the *Write Authorization* column to enable write authorization for the trap recipient (default is disabled). When enabled, a configured user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.

e. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the *Trap Recipient* field. It is recommended the IP address be used.

f. Type a decimal port number in the *UDP Port Number* field to specify the UDP port number

2. Click *Activate* to save the information and close the dialog box.

Configure Threshold Alerts

A threshold alert notifies users when E_Port or F_Port transmit (Tx) or receive (Rx) throughput reaches or exceeds a specified value. Alerts are indicated by:

- An attention indicator (yellow triangle) associated with a port at the *Hardware View*, *Port List View*, or *Port Properties* dialog box.
- Data recorded in the *Threshold Alert Log*.

To configure threshold alerts use the following steps:

1. Select *Threshold Alerts* from the *Configure* menu (*Configure>Threshold Alerts*). The *Configure Threshold Alerts* dialog box appears. If alerts are configured, they display in table format showing the alert name, type, and state.
2. Click *New.* The *New Threshold Alert* dialog box appears (Figure 2-33).

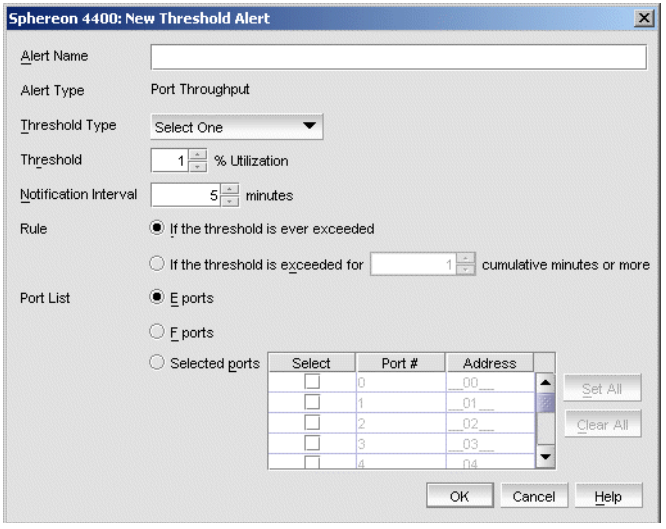


Figure 2-33 New Threshold Alert Dialog Box

3. Type a name (64 alphanumeric characters or less) in the *Threshold Alert Name* field.
4. Select from the *Threshold Type* drop-down list to configure the alert type. Available selections are:

- **Receive -** An alert occurs if the threshold value for receive throughput is reached or exceeded.
- **Transmit -** An alert occurs if the threshold value for transmit throughput is reached or exceeded.
- **Receive and Transmit -** An alert occurs if the threshold value for either throughput is reached or exceeded.

5. Enter a percentage from 1 through 100 in the *Threshold % utilization* field or use the arrow buttons to increase and decrease values. When throughput reaches this percentage of port capacity, a threshold alert occurs.
6. Enter the *Notification interval* in minutes in which throughput is measured and threshold notifications can occur. The valid range is 5 minutes to 70,560 minutes.
7. Select the alert *Rule*
   - Select *If the threshold* is ever exceeded if you want the alert to occur whenever the threshold limit is exceeded.
   - Select *If the Threshold* is exceeded for if you want to specify cumulative minutes that the % utilization should exist during the notification interval before an alert occurs. Enter a value in the field to the right of the selection. The valid range is 1 to the value set for the Notification interval.
8. Either select a Port Type or Selected ports
   - If you *select a Port Type*, the alert generates for all ports configured as the port type you selected.
   - If you *select Selected ports*, you can select individual ports by selecting the check box by each port number or set all ports. Selecting *Set All* places a check mark against the port number. Selecting *Clear All* clears the check marks.
9. Click OK. The Configure Threshold Alerts dialog box appears the name, type, and state of the alert that you just configured.
10. To activate the alert, select the alert information that appears in the Configure Threshold Alerts table and click *Activate*.
11. To deactivate an existing alert, select the alert information that appears in the Configure Threshold Alerts table and click Deactivate.

Enable EFCM Basic Edition and Telnet Access

Follow the procedure in this section to enable EFCM Basic Edition interface and Telnet access through the maintenance port.

To enable EFCM Basic Edition interface and Telnet access through the maintenance port using the Element Manager, use the following steps:

1. Select *Authentication* from the *Security* menu (*Security>Authentication*). The *Configure Authentication* window appears.
2. Select *Enable Web Server/Enable Telnet Access* in the window.
3. Click *Add* to add users who will be permitted to have EFCM Basic Edition interface / Telnet access. The Add/Edit user window appears.
4. Type the *User ID* and *Password* of the user to be added. Confirm the password in the *Retype* field. Click *OK* to return to the *Configure Authentication* Window.
5. Click *Apply*. The *Security Change Confirmation Status - User*s window appears.
6. Click *Start* to apply the settings.

Configure, Enable, and Test E-mail Notification

Follow the procedure in this section to configure, enable, and test e-mail and simple mail transfer protocol (SMTP) addresses to receive event notifications. Configuration and test are performed at the SAN management application. E-mail notification is enabled at the Element Manager application. To perform the procedures:

1. Select *Email* from the *Monitor* menu (Monitor>*Event Notification>Email)*. The *Email Event Notification Setup* dialog box appears (Figure 2-34).

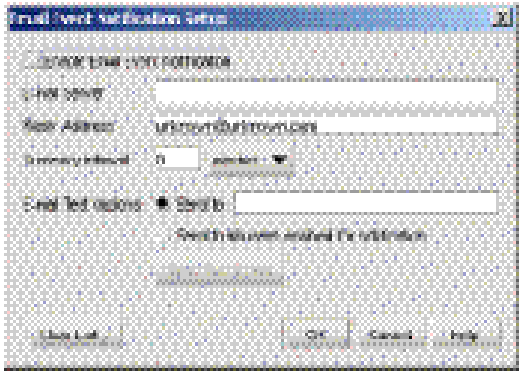


Figure 2-34 Email Event Notification Setup Dialog Box

2. Select *Enable Email Event Notification* check box to enable e-mail transmission to configured addresses.
3. Type the IP address or DNS host name of the SMTP server in the *E-mail Server* field.
4. Type the e-mail address to which replies should be sent in the *Reply Address* field.
5. Type the length of time the application should wait between notifications at the *Summary Interval* field,. Choose **seconds**, **minutes**, or **hours** from the associated drop-down list.
6. Click *User List* to specify users for notification,. The *EFCM Server Users* dialog box appears.
7. Enable the check box in the *Email* column to enable notification for a user. An unchecked box indicates e-mail notification is not enabled.
8. Click *OK* to close the *EFCM Server Users* dialog box.
9. Select the *Send to* radio button (and type recipient IP addresses in the adjacent field) , or select the *Send to all users enabled for notification* radio button at the *E-mail Test Options* field.
10. Click *Send Test Email*. A test message is sent to configured recipients.
11. Click *OK* to save the information and close the dialog box.
12. Maximize the Element Manager application.

13. Select *Enable E-Mail Notification* from the *Maintenance* menu at any view. A check mark appears to indicate e-mail notification for the product is enabled.

NOTE: The enable function must be activated for each product through the Element Manager application.

Configure and Enable Ethernet Events

Perform this procedure to configure and enable Ethernet events. An Ethernet event is recorded (after a user-specified time interval) when the switch-to-management server communication link drops.

To configure and enable Ethernet events, use the following steps:

1. Select *Ethernet Event* from the *Monitor* menu in the EFCM main window. The *Configure Ethernet Events* dialog box appears..
2. Enable the *Enable Ethernet Events* check box. .
3. Type a value between **10** - **120** minutes in the *Ethernet Timeout* field.
4. Click *OK* to close the dialog box.

Configure, Enable, and Test Call-Home Event Notification

Telephone numbers and other information for the call-home feature are configured through the Windows dial-up networking application. Refer to *Task 11: Configure the Call-Home Feature (Optional)* for configuration instructions.

To configure, enable, and test call-home event notification, use the following steps:

NOTE: The call-home feature may not be available if the EFCM Lite application is installed on a customer-supplied platform.

1. Select *Call Home* from the *Monitor* menu *(Monitor>Event Notification>Call Home)* in the EFCM main window. The *Call Home Event Notification Setup* dialog box appears..
2. Enable the *Enable Call Home Event Notification* check box.

NOTE: The enable function must be activated for each product through the Element Manager application.

3. Click *Send Test*. A call-home test message is sent.

4. Click *OK* to close the dialog box.
5. Maximize the Element Manager application.
6. Select *Enable Call Home Notification* from the *Maintenance* menu at any view. A check mark appears to indicate call-home event notification is enabled.

Configure Security

This section describes optional product security features configured through the SAN management or Element Manager applications. The enhanced SANtegrity PFE key must be installed. Refer to *Installing PFE Keys (Optional)* for instructions. Features include:

- **SANtegrity authentication -** Select *SANtegrity Authentication* from the *Configure* menu at the Element Manager application(*Configure>SANtergrity Authentication)*. The *SANtegrity Authentication* dialog box provides five pages (tabs) to configure optional authentication features, including:
  - **Users -** Configure password-protected administrator and operator access to the SAN management and Element Manager applications.
  - **Software -** Configure CHAP-controlled management interface access (out-of-band and inband) to the product.
  - **Devices -** Configure a CHAP secret authentication sequence for nodes (devices) attached to the product through E_Ports or N_ports.
  - **IP Access Control -** Configure a list of device IP addresses or a range of device IP addresses authorized to communicate with the product.
  - **RADIUS Servers -** Configure RADIUS servers. A RADIUS server stores and authenticates passwords and CHAP secrets.
- **Enterprise Fabric Mode -** Use the *Enterprise Fabric Mode* option from the *Configure* menu (*Configure>EFM)* to enable or disable EFM. Fabric binding is activated when EFM is enabled.
- **Fabric binding -** Use the *Fabric Binding* from the *Configure* option from the *Configure* menu (*Configure>Fabric Binding)* to lock parameters of a fabric in accordance with the user configuration. Fabric binding creates a membership list of element (director or switch) Domain_IDs and WWNs that can communicate with the product.

- **Switch binding -** Use the *Switch Binding* option from the *Configure* menu (*Configure>Switch binding)* to create a membership list of node (device) WWNs that can attach to the product. The specified connection policy restricts product access through E_Ports, F_Ports, or in general (all ports).

To configure optional features, refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

Configure Interswitch Links

This section describes ISL performance features configured through the SAN management or Element Manager applications. The OpenTrunking feature requires PFE key installation. Refer to *Installing PFE Keys (Optional)* for instructions. Features include:

- **OpenTrunking -** Use the *OpenTrunking* option from the *Configure* menu (*Configure>Open Trunking*) to optimize ISL bandwidth. The feature monitors data rates (congestion and BB_Credit starvation) through multiple ISLs and load balances traffic (from congested to uncongested links) accordingly.
- **Preferred path -** Use the *Preferred Path* option from the *Configure* menu (*Configure>Preferred Path*) to specify and configure one or more ISL data paths between multiple fabric elements. At each fabric element, a preferred path consists of a source port, exit port, and destination Domain_ID.
- **Port fencing -** Use the *Port Fencing* option from the *Configure* menu (*Configure>Port fencing*) to minimize ISLs that bounce (repeatedly attempt to establish a connection), causing disruptive fabric rebuilds. Fencing defines a bounce threshold that when reached, automatically blocks the disruptive E_Port.

To configure features, refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions. If no additional options or features are to be configured, continue to the next task.

Task 20: Back Up Configuration Data

Follow the procedures in this section to backup server configuration data and create a base restore CD.

Critical configuration data for EFCM is stored on the management server hard drive in the following directories:

- **C:\Program Files\EFCM 8.7\CallHome**
- **C:\Program Files\EFCM 8.7\Client**
- **C:\Program Files\EFCM 8.7\Server.**

The server is configured to automatically mirror the contents of these directories to the CD-RW drive anytime directory contents change or the server is rebooted. The directories contain all SAN management configuration data, log files, firmware versions, call-home and other configuration data; and are used to restore the server operating environment in case of hard drive failure.

The server does not back up Windows operating system data, such as user names, passwords, date and time, and network information. This information was recorded while performing installation tasks, and verified while performing *Task 14: Record or Verify Server Restore Information*.

To back up server configuration data and create a base restore CD:

1. Insert a blank rewritable CD into the CD-RW drive and format the CD:
   a. Locate the *InCD* icon (**1**) at the right side of the task bar at the Windows desktop (Figure 2-35). The icon is indicated by a red down arrow.

Figure 2-35 InCD Icon (Unformatted CD)

   b. Right-click the icon and select *Format (F)*. The first window of the *InCD* wizard appears.

c. Click *Next* to proceed to the second window of the *InCD* wizard. Use default parameters displayed at each window, and click *Next* and *Finish* as appropriate to complete the CD formatting task.

d. When the rewritable CD is formatted, the red down arrow associated with the *InCD* icon changes to a green up arrow.

2. Back up the product configuration file to the server. For instructions, refer to *Back Up Configuration*.

3. Close the Element manager application and return to the EFCM management application.

4. Close the EFCM by selecting *Shutdown* from the *SAN* menu. A *EFCM Message* dialog box appears. Click *Yes* to close the application.

5. Reboot the server to cause directory contents to be written to the blank CD:

   a. Restart Windows. During the reboot process, the LAN connection between the server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error.

   b. Click *Login again* after the management server reboots. The *VNC Authentication* screen appears.

   c. Type the default password and click *OK*. The *Welcome to Windows* dialog box appears.

   d. Type the default password and click *OK*. The *Welcome to Windows* dialog box appears.

   NOTE: The default TightVNC viewer password is **password.**

   e. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the server desktop. The *Log On to Windows* dialog box appears.

   NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the server.

   f. Type the default Windows user name and password and click *OK*. The server's Windows desktop opens and the *EFCM Log In* dialog box appears.

NOTE: The default Windows user name is **Administrator** and the default password is **password**. Both are case-sensitive.

g. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default user ID is **Administrator** and the default password is **password.** Both are case-sensitive.

6. Click *Login*. The application opens and the EFCM main window appears.
7. Remove the base restore CD from the CD-RW drive and store in a safe location. Insert a blank rewritable CD into the CD-RW drive and format the CD. Refer to step 1 for formatting instructions.
8. Go to *Task 21: Cable Fibre Channel Ports*.

Task 21: Cable Fibre Channel Ports

Follow the procedures in this section to cable Fibre Channel ports and connect devices.

To cable Fibre Channel ports and connect devices, use the following steps:

1. Route fiber-optic jumper cables from customer-specified Fibre Channel devices, FC-AL devices, or fabric elements to product ports.
2. Connect device cables to SFP optical port transceivers as directed by the customer.
3. Perform one of the following:
   - If the product is installed on a table or desktop, bundle and secure Fibre Channel cables as directed by the customer.
   - If the product is installed in a customer-supplied equipment rack, bundle Fibre Channel cables from the product and other equipment (groups of 16 maximum), and secure them as directed by the customer.

- If the product is installed in a Fabricenter equipment cabinet, bundle Fibre Channel cables from the product and other equipment (groups of 16 maximum), and secure them in the cable management area at the front-left side of the cabinet.

Task 22: Configure Zoning (Optional)

Perform this procedure to configure, change, add, or delete zones; and to configure, change, enable, or disable zone sets.

- **Zone -** A zone is a group of devices that can access each other through port-to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot.
- **Zone set -** A zone set is a group of zones that is activated or deactivated as a single entity across all managed products in either a single switch or a multiswitch fabric. Only one zone set can be active at one time.

The following naming conventions apply to zones and zone sets:

- All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.
- The first character of a zone set name must be a letter (**A** through **Z** or **a** through **z**).
- A zone set name cannot contain spaces.
- Valid characters are alphanumerics and the caret (**^**), hyphen (**-**), underscore (_), or dollar (**$**) symbols.
- A zone set name can have a maximum of 64 characters.

If the installation is performed from the EFCM Basic Edition interface, refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions. If the installation is performed from the management server, refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

Task 23: Connect Product to a Fabric Element (Optional)

To provide fabric-attached Fibre channel connectivity for devices connected to the product, connect the product to an expansion port (E_Port) of a fabric element (switch or director). Any switch can be used to form this ISL. To connect the product to a fabric element and create an ISL use the following steps:

1. Ensure that the fabric element is accessible by the EFCM Basic Edition interface or defined to the SAN management application. If the fabric element must be defined, refer to the appropriate switch or director installation manual for instructions.
2. Ensure that the preferred domain ID for the product is unique and does not conflict with the ID of another switch or director participating in the fabric.
   - — If the domain ID must be changed from the EFCM Basic Edition, refer to *Task 4: Configure Product at the EFCM Basic Edition Interface (Optional)*.
   - — If the domain ID must be changed from the management server, refer to *Task 19: Configure the Element Manager Application*.
3. Ensure that the R_A_TOV and E_D_TOV values for the product are identical to the values for all switches or directors participating in the fabric.
   - — If the values must be changed from the EFCM Basic Edition, refer to *Task 4: Configure Product at the EFCM Basic Edition Interface (Optional)*.
   - — If the values must be changed from the management server, refer to *Task 19: Configure the Element Manager Application*.
4. Route a multimode fiber-optic cable from a customer-specified E_Port of the fabric element to the front of the product.
5. Connect the fiber-optic cable to a product port as directed by the customer.
6. If the product is managed through the management server, go to step 7. If the product is managed through EFCM Basic Edition:
   a. Select *Port List* from the *Product* menu at any view. The *Port List View* appears.

b. At the *Port List View*, click the physical port number of the fabric ISL (connected in step 5) in the *Port* column. Physical properties for the port appear in the lower panel of the view.

c. Ensure that the *Operational State* field displays **Online** and the *Reason* field displays **N/A** or is blank. If an ISL segmentation or other problem is indicated, go to *MAP 0000: Start MAP* to isolate the problem. If no problems are indicated, installation tasks are complete.

7. Right-click the product icon at the SAN management application's physical map, then select *Element Manager* from the pop-up menu.
8. Click the *Hardware* tab. The *Hardware View* (Figure 2-25) appears.
9. Double-click the graphical port connector used for the fabric ISL (connected in step 5). The *Port Properties* dialog box appears.
10. Ensure that the *Link Incident* field displays **None**, the *Operational State* field displays **Online**, and the *Reason* field displays **N/A** or is blank. If an ISL segmentation or other problem is indicated, go to *MAP 0000: Start MAP* to isolate the problem. If no problems are indicated, installation tasks are complete.

Task 24: Register with the McDATA Filecenter

To complete the installation, register with the McDATA Filecenter web site to receive e-mail updates and access the following:

- Technical publications.
- Firmware and software upgrades.
- Technical newsletters.
- Release notes.

To register with the Filecenter use the following steps:

1. Open the McDATA home page (**http://mcdata.com**). Select *File Center* from the *Support* menu. The Filecenter home page opens (Figure 2-36).
2. Select (click) the *New User Registration* option at the top of the home page. The Filecenter's *New User Registration* page appears. Use the page to input user information. The following is required:
   - Password.

- Verify password.
- First, middle, and last name.

McDATA
McDATA Filecenter
HOME | DOCUMENTS | MY REQUESTS | MY PROFILE
New User Registration | Login | Help
McDATA File Center Brief Overview.
Need more information? McDATA recognizes that the more data you have, the better able you are to make full use of your SAN technologies. The File Center offers convenient, detailed support materials on all McDATA products. New users must first register to enter the center by clicking on the New User Registration icon and filling out the short registration form. If you are already registered, simply click on Login to enter. Registered users may also login from the Support home page on the right side by clicking Support Login.
Please note that some documents are secured and require prior approval to download. When selecting a document, you will be informed if it is secured and guided through the steps of submitting a request for access with easy-to-follow prompts. You will be notified by email once your request has been reviewed.
© Copyright 2003 McDATA Corp. | Privacy Statement | Email: info@mcdata.com
380 Interlocken Crescent, Broomfield, Colorado 80021 phone: 720-558-8000
i16M2006

Figure 2-36 McDATA Filecenter Home Page

- E-mail address.
- Company.
- Title.
- Telephone and facsimile numbers.

3. Complete fields as required and click *Register*. The registration is complete and Filecenter login information is transmitted to the e-mail address specified.
4. Close the Internet session. If no product problems are indicated, installation tasks are complete.

3 Maintenance Analysis Procedures

This chapter describes maintenance analysis procedures (MAPs) used by service representatives to fault isolate Sphereon 4400 Fabric Switch problems or failures to the field-replaceable unit (FRU) level. MAPs consist of step-by-step procedures that provide information to interpret system events, isolate a failure to a single FRU, remove and replace the failed FRU, and verify product operation.

Factory Defaults

Table 3-1 lists factory defaults for product passwords (customer and maintenance level), and the product's Internet Protocol (IP) address, subnet mask, and gateway address.

Table 3-1 Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Quick Start

Table 3-2 lists and summarizes MAPs. Fault isolation normally begins at *MAP 0000: Start MAP*.

Table 3-2 MAP Summary

MAP	Page
MAP 0000: Start MAP	3-5
MAP 0100: Power Distribution Analysis	3-10
MAP 0200: POST Failure Analysis	3-13
MAP 0300: Loss of Server Communication	3-14
MAP 0400: FRU Failure Analysis	3-24
MAP 0500: Port Failure or Link Incident Analysis	3-26
MAP 0600: Fabric or ISL Problem Analysis	3-38

Table 3-3 lists event codes, corresponding MAP references, and provides a quick start guide if an event code is readily available.

Table 3-3 Event Codes versus Maintenance Action

Event Code	Explanation	Action
011	Login Server database invalid.	Go to MAP 0600.
021	Name Server database invalid.	Go to MAP 0600.
031	SNMP request received from unauthorized community.	Add a community name at the Element Manager.
051	Management Server database invalid.	Go to MAP 0600.
061	Fabric Controller database invalid.	Go to MAP 0600.
062	Maximum interswitch hop count exceeded.	Go to MAP 0600.
063	Remote switch has too many ISLs.	Go to MAP 0600.
064	ESS response from indicated domain ID not received after maximum tries.	No action required.
070	E_Port is segmented.	Go to MAP 0600.

Table 3-3 Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
071	Switch is isolated.	Go to MAP 0600.
072	E_Port connected to unsupported switch.	Go to MAP 0600.
073	Fabric initialization error.	Go to *Collecting Maintenance Data*. (EFCM Basic) or *Collecting Maintenance Data* (Element Manager).
074	ILS frame delivery error threshold exceeded.	Go to *Collecting Maintenance Data*. (EFCM Basic) or *Collecting Maintenance Data* (Element Manager).
075	E_Port segmentation recovery.	No action required.
080	Unauthorized worldwide name.	Go to MAP 0500.
081	Invalid attachment.	Go to MAP 0500
082	Port fenced.	Go to MAP 0600.
083	Port set to inactive state.	Go to MAP 0500
120	Error detected while processing system management command.	Go to *Collecting Maintenance Data*. (EFCM Basic) or *Collecting Maintenance Data* (Element Manager).
121	Zone set activation failed - zone set too large.	Reduce size of zone set and retry.
140	Congestion detected on an ISL.	Go to MAP 0600.
141	Congestion relieved on an ISL.	No action required.
142	Low BB_Credit detected on an ISL.	Go to MAP 0600.
143	Low BB_Credit relieved on an ISL.	No action required.
150	Fabric merge failure.	Go to MAP 0600.
151	Fabric configuration failure.	Go to *Collecting Maintenance Data*. (EFCM Basic) or *Collecting Maintenance Data* (Element Manager).
200	Power supply AC voltage failure.	Go to MAP 0100.
201	Power supply DC voltage failure.	Go to MAP 0100.
203	Power supply AC voltage recovery.	No action required.
204	Power supply DC voltage recovery.	No action required.

Table 3-3 Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
206	Power supply removed.	Replace FRU.
207	Power supply installed.	No action required.
300	Cooling fan propeller failed.	Go to MAP 0400.
301	Cooling fan propeller failed.	Go to MAP 0400.
302	Cooling fan propeller failed.	Go to MAP 0400.
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.
370	Cooling fan status polling temporarily disabled.	Go to MAP 0400.
400	Power-up diagnostic failure.	Go to MAP 0200.
410	Switch reset.	No action required.
411	Firmware fault.	Go to MAP 0200.
412	CTP watchdog timer reset.	Go to *Collecting Maintenance Data*. (EFCM Basic) or *Collecting Maintenance Data* (Element Manager).
421	Firmware download complete.	No action required.
423	CTP firmware download initiated.	No action required.
426	Multiple ECC single-bit errors occurred.	Go to MAP 0400.
433	Non-recoverable Ethernet fault.	Go to MAP 0400.
440	Embedded port hardware failed.	Go to MAP 0400.
442	Embedded port anomaly detected.	No action required.
445	ASIC detected a system anomaly.	No action required.
453	New feature key installed.	No action required.
506	Fibre Channel port failure.	Go to MAP 0500.
507	Loopback diagnostics port failure.	Go to MAP 0500.
508	Fibre Channel port anomaly detected.	No action required.

Table 3-3 Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
510	Optical transceiver hot-insertion initiated.	No action required.
512	Optical transceiver nonfatal error.	Go to MAP 0500.
513	Optical transceiver hot-removal completed.	No action required.
514	Optical transceiver failure.	Go to MAP 0500
515	Optical digital diagnostics warning threshold exceeded.	Go to MAP 0500.
516	Optical digital diagnostics alarm threshold exceeded.	Go to MAP 0500.
523	FL_Port open request failed.	No action required.
524	No AL_PA acquired.	No action required.
525	FL_Port arbitration timeout.	No action required.
581	Implicit incident.	Go to MAP 0500.
582	Bit error threshold exceeded.	Go to MAP 0500.
583	Loss of signal or loss of synchronization.	Go to MAP 0500.
584	Not operational primitive sequence received.	Go to MAP 0500.
585	Primitive sequence timeout.	Go to MAP 0500.
586	Invalid primitive sequence received for current link state.	Go to MAP 0500.
810	High temperature warning (CTP thermal sensor).	Go to MAP 0400.
811	Critically hot temperature warning (CTP thermal sensor).	Go to MAP 0400.
812	CTP card shutdown due to thermal violations.	Go to MAP 0400.
850	Switch shutdown due to CTP thermal violations.	Go to MAP 0400.

MAP 0000: Start MAP

This MAP describes initial fault isolation beginning at the:

- Failed product.

- Browser-capable PC with Internet connectivity to the firmware-resident Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface.
- Rack-mount management server running storage area network (SAN) management and Element Manager applications.
- Product-attached open systems interconnection (OSI) host console.

1

Prior to fault isolation, acquire:

- A system configuration drawing or planning worksheet that includes the location of the product, management interface, other McDATA products, and device connections.
- The internet protocol (IP) address, gateway address, and subnet mask for the product reporting the problem.
- User IDs and passwords.

Continue to the next step.

2

Ensure the product is connected to facility power. Inspect the product for indications of being powered on, such as:

- An illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is the product powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to *MAP 0100: Power Distribution Analysis*. **Exit MAP.**

3

At the failed product, inspect the amber **ERR** LED, amber LEDs associated Fibre Channel ports, and green LEDs on power supply assemblies.

Are amber LEDs illuminated? Are green LEDs on power supply assemblies extinguished?

NO **YES**

↓ A FRU failure, power-on self-test (POST) failure, link incident, interswitch link (ISL) problem, fenced E_Port, or segmented E_Port is indicated. To obtain event codes that identify the failure, **go to step 10.**

4

Is the product management interface (browser PC, management server, or OSI host console) powered on and operational?

NO **YES**

↓ **Go to step 7.**

5

Power on the management interface platform and launch the associated management application:

- **EFCM Basic Edition -** Refer to *Task 4: Configure Product at the EFCM Basic Edition Interface (Optional)* for instructions.
- **SAN management application -** Refer to *Task 6: Unpack, Inspect, and Install the Management Server* and *Access the Management Server Desktop* for instructions.
- **OSI host console -** Refer to documentation supplied with the host system for instructions.

Was the maintenance action successful?

NO **YES**

↓ **Go to step 7.**

6

Inspect the management interface for communication link failure. Observe one of the following:

- A **Page cannot be found**, **Unable to locate the server, HTTP 404 - file not found**, or similar message (browser PC).
- The icon representing the product displays a grey square with an exclamation mark (SAN management application).
- A grey square at the alert panel, a No Link status and reason, and no visible product FRUs (Element Manager *Hardware View*).

Was a failure indication observed?

NO **YES**

↓ Communication between the product and management interface failed. Go to *MAP 0300: Loss of Server Communication*. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

7

Inspect product status at the management interface:

a. For the product reporting the problem:

— **EFCM Basic Edition -** Select *Hardware* from the *Product* menu at any view. The *Hardware View* displays.

— **SAN management application -** At the physical map, right-click the status icon for the product reporting the problem and select *Element Manager* from the pop-up menu. The Element Manager opens and the *Hardware View* displays.

— **OSI host console - Go to step 9.**

b. Inspect the status symbol associated with the product. A yellow triangle (attention indicator) indicates the product is operating in degraded mode. A red diamond (failure indicator) indicates the product is not operational.

c. Inspect simulated Fibre Channel ports for a yellow triangle (attention indicator) that overlays the FRU graphic.

d. Inspect simulated FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Is a failure indicated?

NO **YES**

↓ A FRU failure, power-on self-test (POST) failure, link incident, interswitch link (ISL) problem, fenced E_Port, or segmented E_Port is indicated. To obtain event codes that identify the failure, **go to step 10.**

8

A link incident may have occurred, but the LIN alerts option is not enabled and the yellow triangle (attention indicator) does not appear. Inspect the *Link Incident Log*:

a. For the product reporting the problem:

— **EFCM Basic Edition -** Select *Link Incident* from the *Logs* menu at any view. The *Link Incident Log* displays.

— **Element Manager -** Select *Link Incident Log* from the *Logs* menu at any view. The *Link Incident Log* displays.

b. If a link incident occurred, the port number is listed with one of the following messages.

— **Link interface incident - implicit incident.**

— **Link interface incident - bit-error threshold exceeded.**

— **Link failure - loss of signal or loss of synchronization.**

— **Link failure - not-operational primitive sequence (NOS) received.**

— **Link failure - primitive sequence timeout.**

— **Link failure - invalid primitive sequence received for the current link state.**

Did a listed message appear?

NO **YES**

↓ A Fibre Channel link incident is indicated. Go to *MAP 0500: Port Failure or Link Incident Analysis*. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

9

If an incident occurs on the Fibre Channel link between the product and attached OSI server, a link incident record is generated and sent to the server console using the reporting procedure defined in T11/99-017v0.

Was a link incident record generated and sent to the OSI server?

NO **YES**

↓ A Fibre Channel link incident is indicated. Go to *MAP 0500: Port Failure or Link Incident Analysis*. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

10

Inspect the *Event Log* to obtain failure reason codes:

a. For the product reporting the problem:

   — **EFCM Basic Edition -** Select *Event* from the *Logs* menu at any view. The *Event Log* displays.

   — **Element Manager -** Select *Event Log* from the *Logs* menu at any view. The *Event Log* displays.

b. Record the event code and associated date, time, and severity (*Informational*, *Minor*, *Major*, or *Severe*).

c. If multiple event codes are found, record all codes and severity levels. Record the date, time, and sequence, and determine if all codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

Were one or more event codes found?

NO **YES**

↓ **Go to Table 3-3** to obtain event codes. **Exit MAP.**

Return to step 1 and perform fault isolation again. If this is the second time at this step, perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

MAP 0100: Power Distribution Analysis

This MAP describes fault isolation for the product power distribution system, including defective AC power cords or redundant power supplies. The failure indicator is:

- Failure of the product to power on.
- Event code **200** or **201** observed at the *Event Log* (EFCM Basic Edition or Element Manager interface).

1

Ensure the product is connected to facility power. Inspect the product for indications of being powered on, such as:

- An illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is the product powered on?

YES **NO**

↓ A power distribution problem is indicated. **Go to step 4.**

2

Table 3-4 lists event codes, explanations, and MAP steps.

Table 3-4 MAP 100 Event Codes

Event Code	Explanation	Action
200	Power supply AC voltage failure.	Go to step 3.
201	Power supply DC voltage failure.	Go to step 3.

3

As indicated by visual inspection or event code **200** or **201**, one or both power supplies failed and must be disconnected and replaced. Refer to *RRP 2: Redundant Power Supply*.

- The procedure is concurrent and performed while the product is operational.
- Perform a data collection as part of FRU removal and replacement. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

4

Inspect and verify facility power is within specifications:

- One single-phase connection for each power supply.
- Input power between 100 and 240 VAC, at least 5 amps.
- Input frequency between 50 and 60 Hz.

Is facility power within specifications?

YES **NO**

↓ Ask the customer to correct the facility power problem. When corrected, **continue to the next step.**

5

One or both power supplies are disconnected from facility power, improperly connected, or failed. Verify power supplies are connected to facility power.

a. Ensure AC power cords are connected to the rear of the switch and facility power receptacles. If not, connect power cords as directed by the customer.

b. Ensure facility circuit breakers are on. If not, ask the customer to set breakers on.

c. Ensure AC power cords are not damaged. If damaged, replace the cords.

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

6

Verify power supply operation.

a. Inspect each power supply to determine if the green LED is extinguished.

b. If a green LED is extinguished, ensure the indicated power supply is properly connected. Disconnect and reconnect the power supply.

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

A power supply failure is indicated. **Go to step 3.**

MAP 0200: POST Failure Analysis

This MAP describes fault isolation for a POST failure. The failure indicator is event code **400** or **411** observed at the *Event Log* (EFCM Basic Edition or Element Manager interface).

1

Table 3-5 lists event codes, explanations, and MAP steps.

Table 3-5 MAP 200 Event Codes

Event Code	Explanation	Action
400	Power-up diagnostic failure.	Go to step 2.
411	Firmware fault.	Go to step 4.

2

As indicated by event code **400**, POST/IPL diagnostics detected a FRU failure.

a. At the *Event Log*, examine the first two bytes of event data.

b. Byte **0** specifies failed FRU. Byte **1** specifies the slot number of the failed FRU (**00** for nonredundant, **00** or **01** for redundant) as listed in Table 3-6.

Table 3-6 MAP 200 Byte 0 FRU Codes

Byte 0	Failed FRU	Action
02	CTP card.	Replace the switch. **Exit MAP.**
05	Fan module.	Replace the switch. **Exit MAP.**
06	Power supply.	Go to step 3.

3

A power supply failed POSTs and must be removed and replaced. Refer to *RRP 2: Redundant Power Supply*.

- The procedure is concurrent and performed while the product is operational.
- Perform a data collection as part of FRU removal and replacement. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

4

As indicated by event code **411**, POST/IPL diagnostics detected a firmware failure and performed an online dump. All Fibre Channel ports reset after failure and devices momentarily logout, login, and resume operation. Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

MAP 0300: Loss of Server Communication

This MAP describes fault isolation for the product to browser PC Internet connection (EFCM Basic Edition interface) or the product to management server LAN connection. The failure indicator is:

- A **Page cannot be found**, **Unable to locate the server**, **HTTP 404 - file not found**, or similar message (browser PC).
- The icon representing the product displays a grey square with an exclamation mark (SAN management application).
- A grey square at the alert panel, a **No Link** status and reason, and no visible product FRUs (Element Manager *Hardware View*).

NOTE: Upon restart, it may take up to five minutes for the management interface logical connection to activate. This delay is normal.

1

The following product management interface failed:

- EFCM Basic Edition (browser PC). **Go to step 2.**
- SAN management or Element Manager application (management server). **Go to step 5.**

2

A **Page cannot be found**, **Unable to locate the server**, **HTTP 404 - file not found**, or similar message appears at the browser PC, indicating the PC cannot communicate with the product because:

- The product-to-PC Internet link could not be established.
- AC power distribution for the product failed or AC power was disconnected.
- The product CTP card failed.

Continue to the next step.

3

Ensure the product is connected to facility power. Inspect the product for indications of being powered on, such as:

- An illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is the product powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to *MAP 0100: Power Distribution Analysis*. **Exit MAP.**

4

A product-to-PC link problem (Internet too busy or IP address typed incorrectly) or an Ethernet port failure is indicated.

a. Wait approximately five minutes, then attempt to login to the product.

b. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the product IP address obtained in *MAP 0000: Start MAP*. The *Username and Password Required* dialog box appears.

c. Type the user name and password obtained in *MAP 0000: Start MAP* and click *OK*. If the EFCM Basic Edition interface does not open, wait five minutes and perform this step again.

Is the EFCM Basic Edition interface operational?

NO **YES**

↓ The Internet connection is restored. **Exit MAP.**

Failure of the Ethernet port is indicated. Replace the switch. **Exit MAP.**

5

A status icon (grey square with yellow exclamation mark) appears at the SAN management application, indicating the management server cannot communicate with the product because:

- The server-to-PC Internet link could not be established.
- AC power distribution for the product failed or AC power was disconnected.
- The product CTP card failed.

Continue to the next step.

6

Ensure the product is connected to facility power. Inspect the product for indications of being powered on, such as:

- An illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is the product powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to *MAP 0100: Power Distribution Analysis*. **Exit MAP.**

7

At the SAN management application's physical map, right-click the status icon for the product reporting the problem and select *Element Manager* from the pop-up menu. The Element Manager opens and the *Hardware View* displays:

- A grey square appears at the alert panel.

- No product FRUs are visible.
- The *Status* table is yellow, the *Status* field displays **No Link**, and the **Reason** field displays an error message listed in Table 3-7.

Table 3-7 MAP 300 Error Messages

Error Message	Action
Never connected.	Go to step 8.
Link timeout.	Go to step 8.
Protocol mismatch.	Go to step 15.
Duplicate session.	Go to step 18.
Unknown network address.	Go to step 21.
Incorrect product type.	Go to step 23.

8

Transmit or receive errors for the Ethernet adapter exceeded a threshold, the link was not connected, or the link timed out. A problem with the Ethernet cable, Ethernet hub(s), or other LAN-attached device is indicated. Verify the product is connected to the management server through one or more Ethernet hubs:

a. Ensure an RJ-45 Ethernet cable connects the product to a hub. If not, connect the cable as directed by the customer.

b. Ensure an RJ-45 Ethernet cable connects the management server to a hub. If not, connect the cable as directed by the customer.

c. Ensure Ethernet cables are not damaged. If damaged, replace the cables.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

9

Does the configuration use multiple daisy-chained Ethernet hubs?

YES **NO**

↓ **Go to step 11.**

10

Verify hubs are correctly daisy-chained.

a. **Top hub -** As shown in Figure 3-1 (**1**), ensure an RJ-45 Ethernet cable connects to port **24** and the medium-dependent interface (MDI) switch is set to **MDI** (in).

b. **Middle hub -** As shown in Figure 3-1 (**2**), ensure the cable from the top hub connects to port **12,** the cable from the bottom hub connects to port **24**, and the MDI switch is set to **MDI** (in).

c. **Bottom hub -** As shown in Figure 3-1 (**3**), ensure the cable from the middle hub connects to port **12** and the MDI switch is set to **MDIX** (out).

Figure 3-1 Daisy-Chained Ethernet Hubs

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

11

Verify operation of Ethernet hub(s). Inspect each hub for indications of being powered on, such as:

- Green **Power** LED illuminated.
- Green **Status** LEDs illuminated.

Is a failure indicated?

YES **NO**

↓ **Go to step 13.**

12

Remove and replace the Ethernet hub. Refer to supporting documentation for instructions.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

13

A problem with LAN-attached device is indicated.

- If the problem is associated with another fabric element or management server, go to *MAP 0000: Start MAP* to isolate the problem for that product. **Exit MAP.**
- If the problem is associated with an unrelated device, inform the customer for problem resolution.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

14

The Ethernet adapter on the product CTP card reset in response to an error. The connection to the management server terminated briefly, then recovered upon reset. Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

15

A protocol mismatch occurred because the SAN management application and the product firmware are not at compatible release levels. Recommend to the customer the downlevel version (software or firmware) be upgraded.

Does the SAN management application require upgrade?

YES **NO**

↓ **Go to step 17.**

16

Upgrade the SAN management application. Refer to *Installing or Upgrading Software*.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

17

Product firmware upgrade is required. Refer to *Upgrading Firmware* (EFCM Basic Edition) or *Upgrading Firmware* (Element Manager). Perform a data collection after the upgrade. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

18

An instance of the SAN management application is open at another management server and communicating with the product (duplicate session). Inform the customer and either:

- Power off the server running the second instance of the application.
- Configure the server running the second instance of the application as a client workstation.

Does the customer want the second server configured as a client?

YES **NO**

↓ Power off the server reporting the **Duplicate Session** problem. **Exit MAP.**

19

Determine the IP address of the management server running the first instance of the SAN management application.

a. After the server powers on and successfully completes POSTs, the LCD panel displays a **Welcome!!** message and continuously cycles through and displays operational information.

b. After a few seconds, the LCD panel displays a **LAN 2: 010.001.001.001** message.

c. Depending on product-to-server LAN connectivity, record the appropriate IP address (**LAN 1** or **LAN 2**).

Continue to the next step.

20

Configure the management server reporting the **Duplicate Session** problem as a client.

a. At the SAN management application, select *Logout* from the *SAN* menu. The application closes and the *Log In* dialog box displays.

b. Type the user ID and password obtained in *MAP 0000: Start MAP*. Both are case sensitive).

c. Type the IP address of the management server running the first instance of the SAN management application in the *Network Address* field.

d. Click *Login*. The application opens and the main window displays.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored and the second management server is a client. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

21

The IP address defining the product to the SAN management application is incorrect or unknown and must be verified. An asynchronous RS-232 modem cable and maintenance terminal (desktop or notebook PC) with a Windows-based operating system and RS-232 serial communication software (such as ProComm Plus or HyperTerminal) are required. To verify the IP address:

a. Using a Phillips screwdriver, remove the protective cap from the 9-pin maintenance port at the rear of the chassis. Connect one end of the RS-232 modem cable to the port.

b. Connect the other cable end to a 9-pin serial communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.

c. Power on the maintenance terminal. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.

d. At the *Windows Workstation* menu, sequentially select the *Programs*, *Accessories*, *Communications*, and *HyperTerminal* options. The *Connection Description* dialog box displays.

e. Type a descriptive product name in the *Name* field and click *OK*. The *Connect To* dialog box displays.

f. Ensure the *Connect using* field displays **COM1** or **COM2** (depending on the port connection to the product), and click *OK*. The *COMn Properties* dialog box displays, where *n* is **1** or **2**.

g. Configure *Port Settings* parameters:

   — *Bits per second* - **115200**.

   — *Data bits* - **8**.

   — *Parity* - **None**.

   — *Stop bits* - **1**.

   — *Flow control* - **Hardware** or **None**.

   Click *OK*. The *New Connection - HyperTerminal* window displays.

h. At the **>** prompt, type the user password (default is **password**) and press **Enter**. The password is case sensitive. The *New Connection - HyperTerminal* window displays with software and hardware version information for the product, and a **C >** prompt at the bottom of the window.

i. At the **C >** prompt, type the **ipconfig** command and press **Enter**. The *New Connection - HyperTerminal* window displays with configuration information listed.

j. Record the product IP address.

k. Select *Exit* from the *File* pull-down menu. A HyperTerminal message box appears.

l. Click *Yes*. A second message box appears. Click *No* to exit and close the application.

m. Power off the maintenance terminal and disconnect the modem cable. Replace the protective cap over the maintenance port.

Continue to the next step.

22

Define the product IP address (determined in step 21) to the management server.

a. At the SAN management application, select *Setup* from the *Discover* menu. The *Discover Setup* dialog box displays.

b. Ensure the product to be reconfigured is moved from the *Selected Individual Addresses* list to the *Available Addresses* list. Select (highlight) the product and click *Edit*. The *Address Properties* dialog box displays with the *IP Address* page open.

c. Type the correct product IP address in the *IP Address* field.

d. Move the reconfigured product from the *Available Addresses* list to the *Selected Individual Addresses* list.

e. Click *OK* to save the address, close the dialog box, and redefine the product to the SAN management application.

f. Click *OK* to close the *Discover Setup* dialog box.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

23

An incorrect product type is defined to the management server.

a. At the SAN management application, select *Setup* from the *Discover* menu. The *Discover Setup* dialog box displays.

b. Ensure the incorrect product (to be deleted) is moved from the *Selected Individual Addresses* list to the *Available Addresses* list. Select (highlight) the product and click *Delete*. The product is deleted.

c. Click *Add*. The *Address Properties* dialog box displays with the *IP Address* page open.

d. Type a product description in the *Description* field.

e. Type the product IP address (determined by the network administrator) in the *IP Address* field.

f. Type the product subnet mask (determined by the network administrator) in the *Subnet Mask* field.

g. Click the *Product Type and Access* tab. Select *Switch* from the *Product Type* drop-down list and type customer-specified values in the *User ID*, *Password*, and *Retype Password* fields.

h. Click *OK* to close the dialog box and define the new product configuration to the SAN management application.

i. Click *OK* to close the *Discover Setup* dialog box.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

MAP 0400: FRU Failure Analysis

This MAP describes fault isolation for product FRUs. The failure indicator is:

- Illumination of the associated amber LED.
- Event code **300**, **301**, **302**, **370**, **426**, **433**, **440**, **810**, **811**, **812**, or **850** observed at the *Event Log* (EFCM Basic Edition or Element Manager interface).

1

Table 3-8 lists event codes, explanations, and MAP steps.

Table 3-8 MAP 400 Event Codes

Event Code	Explanation	Action
300	Cooling fan propeller failed.	Go to step 2.
301	Cooling fan propeller failed.	Go to step 2.
302	Cooling fan propeller failed.	Go to step 2.
370	Cooling fan status polling temporarily disabled.	Go to step 3.
426	Multiple ECC single-bit errors occurred.	Go to step 4.
433	Non-recoverable Ethernet fault.	Go to step 5.
440	Embedded port hardware failed.	Go to step 5.
810	High temperature warning (CTP thermal sensor).	Go to step 6.
811	Critically hot temperature warning (CTP thermal sensor).	Go to step 6.
812	CTP card shutdown due to thermal violations.	Go to step 6.
850	Switch shutdown due to CTP thermal violations.	Go to step 6.

2

Visual inspection or event code **300**, **301**, or **302** indicates one or more cooling fans failed. Replace the switch. **Exit MAP.**

3

As indicated by event code **370**, cooling fan status polling is temporarily disabled and status values for one or more fans exceed a set threshold. This indicates possible fan degradation or failure.

Is this event code a recurring problem?

NO **YES**

↓ A fan failure is indicated. **Go to step 2.**

Monitor fan operation or recording of additional failure event codes. **Exit MAP.**

4

As indicated by event code **426**, an intermittent synchronous dynamic random access memory (SDRAM) problem may result in switch failure.

Is this event code a recurring problem?

NO **YES**

↓ A CTP card failure is indicated. Replace the switch. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

5

As indicated by event code **433** or **440**, the CTP card failed. Replace the switch. **Exit MAP.**

6

As indicated by event code **810**, **811**, **812**, or **850**, an intermittent thermal problem may result in switch failure. Reset the product. Refer to *IML or Reset Switch* for instructions.

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

A CTP card failure is indicated. Replace the switch. **Exit MAP.**

MAP 0500: Port Failure or Link Incident Analysis

This MAP describes fault isolation for small form factor pluggable (SFP) optical transceivers and Fibre Channel link incidents. The failure indicator is:

- Event code **080**, **081**, **083**, **506**, **507**, **512**, **514**, **515**, or **516** observed at the *Event Log* (EFCM Basic Edition or Element Manager interface).
- Event code **581**, **582**, **583**, **584**, **585**, or **586** observed at the console of an OSI server attached to the product reporting the problem.
- An error message observed at the *Link Incident Log* (EFCM Basic Edition or Element Manager interface).

1

Table 3-9 lists event codes, explanations, and MAP steps.

Table 3-9 MAP 500 Event Codes

Event Code	Explanation	Action
080	Unauthorized worldwide name.	Go to step 2.
081	Invalid attachment.	Go to step 3.
083	Port set to inactive state.	Go to step 13.
506	Fibre Channel port failure.	Go to step 17.
507	Loopback diagnostics port failure.	Go to step 18.
512	Optical transceiver nonfatal error.	Go to step 17.
514	Optical transceiver failure.	Go to step 17.
515	Optical digital diagnostics warning threshold exceeded.	Go to step 17.
516	Optical digital diagnostics alarm threshold exceeded.	Go to step 17.
581	Implicit incident.	Go to step 19.
582	Bit error threshold exceeded.	Go to step 19.
583	Loss of signal or loss of synchronization.	Go to step 19.
584	Not operational primitive sequence received.	Go to step 19.
585	Primitive sequence timeout.	Go to step 19.
586	Invalid primitive sequence received for current link state.	Go to step 19.

Table 3-10 lists link incident messages and MAP steps.

Table 3-10 Link Incident Messages

Explanation	Action
Link interface incident - implicit incident.	Go to step 19.
Link interface incident - bit-error threshold exceeded.	Go to step 19.
Link failure - loss of signal or loss of synchronization.	Go to step 19.

Table 3-10 Link Incident Messages (Continued)

Explanation	Action
Link failure - not-operational primitive sequence (NOS) received.	Go to step 19.
Link failure - primitive sequence timeout.	Go to step 19.
Link failure - invalid primitive sequence received for current link state.	Go to step 19.

2

As indicated by event code **080**, the eight-byte (16-digit) worldwide name (WWN) is not valid or an unconfigured nickname was used.

a. For the product reporting the problem:
   - **EFCM Basic Edition -** Select *Node List* from the *Product* menu at any view. The *Node List View* displays.
   - **Element Manager -** Select the *Node List* tab at any view. The *Node List View* displays.

b. At the *Port WWN* column, inspect the WWN assigned to the port or attached device.

c. The WWN must be entered in (***XX:XX:XX:XX:XX:XX:XX:XX***) format or must be a valid nickname. Ensure a valid WWN or nickname is entered.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

3

As indicated by event code **081**, a port has an invalid attachment.

a. At the *Event Log*, examine the first five bytes of event data.

b. Byte **0** specifies the port reporting the problem. Byte **4** specifies the invalid attachment reason as listed in Table 3-11.

Table 3-11 **Invalid Attachment Reasons and Actions**

Byte 4	Invalid Attachment Reason	Action
01	Unknown	Contact the next level of support.
02	ISL connection not allowed.	Go to step 4.
03, 04	Incompatible switch.	Go to step 5.
05	Loopback plug connected.	Go to step 6.
06	N-Port connection not allowed.	Go to step 4.
07	Non-McDATA switch at other end.	Go to step 5.
08	E_Port capability disabled.	Go to step 7.
0A	Unauthorized port binding WWN.	Go to step 2.
0B	Unresponsive node.	Go to step 8.
0C	ESA security mismatch.	Go to step 10.
0D	Fabric binding mismatch.	Go to step 11.
0E	Authorization failure reject.	Go to step 8.
0F	Unauthorized switch binding WWN.	Go to step 10.
10	Authentication failure	Go to step 12.
11	Fabric mode mismatch.	Go to step 5.

4

A connection is not allowed because of a conflict with the configured port type. An expansion port (E_Port) is cabled to a Fibre Channel device or a fabric port (F_Port) is cabled to a director or fabric switch.

a. For the product reporting the problem:

— **EFCM Basic Edition -** Select *Ports* and *Basic Info* from the *Configure* menu at any view. The *Basic Information View* displays.

— **Element Manager -** Select *Ports* from the *Configure* menu at any view. The *Configure Ports* dialog box displays.

b. If necessary, use the vertical scroll bar to display the information row for the port indicating an invalid attachment.

c. Select (click) the *Type* field and configure the port as follows:

- Select fabric port (**F_Port**) if the port is cabled to a device.
- Select expansion port (**E_Port**) if the port is cabled to a director or switch (ISL).

d. Click *OK* or *Activate*.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

5

An ISL connection is not allowed because one of the following mode-mismatch conditions was detected:

- The product is configured to operate in **Open Fabric 1.0** mode and is connected to a fabric element not configured to **Open Fabric 1.0** mode.
- The product is configured to operate in **Open Fabric 1.0** mode and is connected to a legacy McDATA switch at the incorrect exchange link parameter (ELP) revision level.
- The product is configured to operate in **Open Fabric 1.0** mode and is connected to a non-McDATA switch at the incorrect ELP revision level.
- The product is configured to operate in **McDATA Fabric 1.0** mode and is connected to a non-McDATA switch.

Reconfigure the operating mode:

a. Set the product offline. Refer to *Setting Online State* (EFCM Basic Edition) or *Setting Online State* (Element Manager).

b. For the product reporting the problem:

— **EFCM Basic Edition -** Select *Switch* and *Fabric Parameters* from the *Configure* menu at any view. The *Fabric Parameters View* displays.

— **Element Manager -** Select *Operating Parameters* and *Fabric Parameters* from the *Configure* menu at any view. The *Configure Fabric Parameters* dialog box displays.

c. Select **McDATA Fabric 1.0** or **Open Fabric 1.0** from the *Interop Mode* drop-down list.

   — Select **McDATA Fabric 1.0** if the product is attached *only* to other McDATA directors or switches operating in **McDATA Fabric 1.0** mode.

   — Select **Open Fabric 1.0** if the product is attached to directors or switches produced by open-fabric compliant original equipment manufacturers (OEMs).

d. Click *OK* or *Activate*.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

6

A loopback (wrap) plug is connected to the port with no diagnostic running. Remove the plug from the port receptacle. If directed by the customer, connect a fiber-optic jumper cable attaching a device to the product.

- If the port is operational with no device attached, both LEDs adjacent to the port extinguish and the port state is *No Light*.
- If the port is operational with a device attached, the green LED illuminates, the amber LED extinguishes, and the port state is *Online*.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

7

An ISL connection is not allowed because E_Port capability is disabled. Install the full-fabric PFE key to enable E_port capability. Refer to *Installing PFE Keys (Optional)* (EFCM Basic Edition) or *Task 16: Configure PFE Key (Optional)* (Element Manager). **Exit MAP.**

8

The connection timed out because of an unresponsive device or an ISL security violation (authorization failure reject). Check port status and clean fiber-optic components.

a. Inform the customer the port will be blocked. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

b. Block the port. Refer to *Blocking or Unblocking a Port* (EFCM Basic Edition) or *Blocking or Unblocking a Port* (Element Manager).

c. Clean fiber-optic connectors. Refer to *Clean Fiber-Optic Components*.

d. Unblock the port. Refer to *Blocking or Unblocking a Port* (EFCM Basic Edition) or *Blocking or Unblocking a Port* (Element Manager).

e. Monitor port operation for approximately five minutes.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

9

Inspect and service host bus adapters (HBAs).

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

10

A connection is not allowed because of a switch binding or exchange security attribute (ESA) feature mismatch. Switch binding parameters must be compatible for both fabric elements. At the EFCM Basic Edition interface or Element Manager, ensure switch binding is enabled, the connection policy is compatible, and switch membership lists are compatible for both elements.

- **EFCM Basic Edition -** Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.

- **Element Manager -** Refer to the *McDATA Sphereon 4400 Fabric Switch Element Manager User Manual* (620-000241) for instructions.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

11

A connection is not allowed because of a fabric binding mismatch. Fabric membership lists must be compatible for both elements. At the EFCM Basic Edition interface or SAN management application, ensure fabric binding is enabled and fabric membership lists are compatible for both elements.

- **EFCM Basic Edition -** Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.
- **SAN management application -** Refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

12

A connection is not allowed because of a SANtegrity authentication failure. At the EFCM Basic Edition interface or Element Manager, modify the IP address access control list, product-level authentication settings, port-level authentication settings, and challenge handshake authentication protocol (CHAP) sequence to ensure device access to the product.

- **EFCM Basic Edition -** Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.
- **Element Manager -** Refer to the *McDATA Sphereon 4400 Fabric Switch Element Manager User Manual* (620-000241) for instructions.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

13

As indicated by event code **083**, a port is set to an inactive state.

a. At the *Event Log*, examine the first two bytes of event data.

b. Byte **0** specifies the port reporting the problem. Byte **1** specifies the inactive reason as listed in Table 3-12.

Table 3-12 Inactive Port Reasons and Actions

Byte 1	Inactive Port Reason	Action
02	Feature key not enabled.	Go to step 14.
03	Switch speed conflict.	Go to step 15.
04	Optics speed conflict.	Go to step 15.
06	Port swap conflict.	Go to step 16.

14

A port is inactive because Flexport Technology is disabled. Install the Flexport Technology PFE key to enable N_Port capability. Refer to *Installing PFE Keys (Optional)* (EFCM Basic Edition) or *Task 16: Configure PFE Key (Optional)* (Element Manager). **Exit MAP.**

15

A port is inactive because the:

- Port cannot operate at the product (backplane) speed.
- Optical transceiver does not support the configured port speed.

Change the port speed to be compatible with the backplane or optical transceiver speed.

a. For the product reporting the problem:

— **EFCM Basic Edition -** Select *Ports* and *Basic Info* from the *Configure* menu at any view. The *Basic Information View* displays.

— **Element Manager -** Select *Ports* from the *Configure* menu at any view. The *Configure Ports* dialog box displays.

b. If necessary, use the vertical scroll bar to display the information row for the inactive port.

c. Select (click) the *Speed* field and configure the port.

d. Click *OK* or *Activate*.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

16

A port is inactive because the port swap configuration is invalid. Perform a port swap procedure (Element Manager only), ensure the configuration is valid, and ensure the port address matches the hardware configuration definition (HCD) of the attached host. Refer to *Swap Ports*. **Exit MAP.**

17

As indicated by event codes **506**, **512**, **514**, **515**, or **516**, a port failed and the optical transceiver must be removed and replaced. Refer to *RRP 1: SFP Optical Transceiver*.

- The procedure is concurrent and performed while the product is operational.
- Replace the transceiver with a transceiver of the same speed.
- Perform an external loopback test. Refer to *External Loopback Test* (EFCM Basic Edition) or *External Loopback Test* (Element Manager).

NOTE: Event code **514** may generate a call-home event that incorrectly indicates a CTP card failure. Although the optical socket on the CTP card may have failed, replace the transceiver and verify operation. If a failure is still indicated, replace the switch. When event code **514** is indicated, ensure a replacement transceiver and switch are available.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

18

As indicated by event code **507**, a port failed a loopback test. Reset the failed port.

a. At the EFCM Basic Edition interface:

   1. Select *Ports* and *Reset* from the *Maintenance* menu at any view. The *Reset View* displays.
   2. If necessary, use the vertical scroll bar to display the information row for the port.
   3. Select (click) the check box in the *Reset* column.
   4. Click *OK*. The port resets.

b. At the Element Manager:

   1. At the *Hardware View*, right-click the port. A pop-up menu appears.
   2. Select *Reset Port*. The message **This operation will cause a link reset to be sent to the attached device** displays.
   3. Click *OK*. The port resets.

c. Perform an external loopback test for the reset port. Refer to *External Loopback Test* (EFCM Basic Edition) or *External Loopback Test* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Go to step 17.

19

A message appeared in the *Link Incident Log* or an event code **581**, **582**, **583**, **584**, **585**, or **586** was observed at the console of an OSI server attached to the product reporting the problem. Clear the link incident (Element Manager only).

a. At the *Hardware View*, right-click the port. A pop-up menu appears.

b. Select *Clear Link Incident Alert(s)*. The *Clear Link Incident Alert(s)* dialog box displays.

c. Select the *This port (**n**) only* radio button and click *OK*. The link incident clears.

d. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The problem is transient and the product port is operational. **Exit MAP.**

20

Clean fiber-optic components.

a. Inform the customer the port will be blocked. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

b. Block the port. Refer to *Blocking or Unblocking a Port* (EFCM Basic Edition) or *Blocking or Unblocking a Port* (Element Manager).

c. Clean fiber-optic connectors. Refer to *Clean Fiber-Optic Components*.

d. Unblock the port. Refer to *Blocking or Unblocking a Port* (EFCM Basic Edition) or *Blocking or Unblocking a Port* (Element Manager).

e. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The product port is operational. **Exit MAP.**

21

Disconnect the fiber-optic jumper cable from the port and connect the cable to a spare port.

Is a link incident reported at the new port?

YES **NO**

↓ The port reporting the problem is causing the link incident. This indicates port degradation and a possible pending failure. **Go to step 17.**

22

Ensure the attached fiber-optic jumper cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

a. Inform the customer the port will be blocked. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

b. Block the port. Refer to *Blocking or Unblocking a Port* (EFCM Basic Edition) or *Blocking or Unblocking a Port* (Element Manager).

c. Remove and replace the fiber-optic jumper cable.

d. Unblock the port. Refer to *Blocking or Unblocking a Port* (EFCM Basic Edition) or *Blocking or Unblocking a Port* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

23

The attached device is causing the recurrent link incident. Inform the customer of the problem and have the system administrator:

a. Inspect and verify operation of the attached device.

b. Repair the attached device if a failure is indicated.

c. Monitor port operation for approximately five minutes.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

MAP 0600: Fabric or ISL Problem Analysis

This MAP describes fault isolation for fabric, interswitch link (ISL), fenced E_Port, and segmented E_Port problems. The failure indicator

is an event code **011**, **021**, **051**, **061**, **062**, **063**, **070**, **071**, **072**, **082**, **140**, **142**, or **150** observed at the *Event Log* (EFCM Basic Edition or Element Manager interface).

1

Table 3-13 lists event codes, explanations, and MAP steps.

Table 3-13 MAP 600 Event Codes

Event Code	Explanation	Action
011	Login Server database invalid.	Go to step 2.
021	Name Server database invalid.	Go to step 2.
051	Management Server database invalid.	Go to step 3.
061	Fabric Controller database invalid.	Go to step 4.
062	Maximum interswitch hop count exceeded.	Go to step 5.
063	Remote switch has too many ISLs.	Go to step 6.
070	E_Port is segmented.	Go to step 7.
071	Switch is isolated.	Go to step 7.
072	E_Port connected to unsupported switch.	Go to step 15.
082	Port fenced.	Go to step 16.
140	Congestion detected on an ISL.	Go to step 21.
142	Low BB_Credit detected on an ISL.	Go to step 21.
150	Fabric merge failure.	Go to step 22.

2

A minor error occurred that caused the Fabric Services database to be re-initialized to an empty state, and a disruptive fabric logout and login occurred for all attached devices. Indications are:

- **Event code 011 -** The Login Server database failed cyclic redundancy check (CRC) validation.
- **Event code 021 -** The Name Server database failed CRC validation.

Devices resume operation after fabric login. Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

3

As indicated by event code **051**, a minor error occurred that caused the Management Server database to be re-initialized to an empty state and fail CRC validation. A disruptive server logout and login occurred for all attached devices.

Devices resume operation after Management Server login. Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

4

As indicated by event code **061**, a minor error occurred that caused the Fabric Controller database to be re-initialized to an empty state and fail CRC validation. The product briefly lost interswitch link capability.

Interswitch links resume operation after CTP reset. Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

5

As indicated by event code **062**, Fabric Controller software detected a path to another fabric element (director or switch) that traverses more than three interswitch links (hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and reconfigure the fabric so the path between any two fabric elements does not traverse more than three hops.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

6

As indicated by event code **063**, Fabric Controller software detected:

- A fabric element with more than 32 ISLs (SAN management application Version 3.2 or earlier).
- A fabric element with more than 128 ISLs (SAN management application Version 3.3 or later).

Fibre Channel frames may be lost or directed in loops because of potential fabric routing problems. Advise the customer of the problem and reconfigure the fabric so that no directors or switches have more than the proscribed number of ISLs.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

7

Event code **070** indicates an E_Port detected an incompatibility with an attached fabric element, segmented the port, and prevented fabric participation. A segmented E_port cannot transmit Class 2 or Class 3 Fibre Channel traffic. Event code **071** indicates the product is isolated from all fabric elements, and is accompanied by an event code **070** for each segmented E_Port. Event code **071** is resolved when all **070** events are corrected. Obtain supplementary event data as follows:

a. At the *Event Log*, examine the first five bytes of event data.

b. Byte **0** specifies the segmented E_port. Byte **4** specifies the segmentation reason as listed in Table 3-14. The reason also displays at the *Port List View* (EFCM Basic Edition) or *Port Properties* dialog box (Element Manager).

Table 3-14 E_Port Segmentation Reasons and Actions

Byte 4	Segmentation Reason	Action
01	Incompatible operating parameters.	Go to step 8.
02	Duplicate domain ID.	Go to step 9.
03	Incompatible zoning configurations.	Go to step 10.
04	Build fabric protocol error.	Go to step 11.
05	No principal switch.	Go to step 13.
06	No response from attached switch (hello timeout).	Go to step 14.

8

An E_Port segmented because the error detect time out value (E_D_TOV) or resource allocation time out value (R_A_TOV) is incompatible with the attached fabric element.

a. Contact customer support or engineering personnel to determine the recommended E_D_TOV and R_A_TOV values for both fabric elements.

b. Inform the customer both products will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

c. Set both products offline. Refer to *Setting Online State* (EFCM Basic Edition) or *Setting Online State* (Element Manager).

d. For the first product reporting the problem:

— **EFCM Basic Edition -** Select *Switch* and *Fabric Parameters* from the *Configure* menu at any view. The *Fabric Parameters View* displays.

— **Element Manager -** Select *Operating Parameters* and *Fabric Parameters* from the *Configure* menu at any view. The *Configure Fabric Parameters* dialog box displays.

e. Type the recommended E_D_TOV and R_A_TOV values, then click *OK* or *Activate*.

f. Repeat steps **d** and **e** at the second product (attached to the segmented E_Port). Use the same E_D_TOV and R_A_TOV values.

g. Set both products online. Refer to *Setting Online State* (EFCM Basic Edition) or *Setting Online State* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

9

An E_Port segmented because two fabric elements had duplicate domain IDs.

a. Determine the desired domain ID (**1** through **31** inclusive) for each product.

b. Inform the customer both products will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

c. Set both products offline. Refer to *Setting Online State* (EFCM Basic Edition) or *Setting Online State* (Element Manager).

d. For the first product reporting the problem:

   — **EFCM Basic Edition -** Select *Switch* and *Parameters* from the *Configure* menu at any view. The *Parameters View* displays.

   — **Element Manager -** Select *Switch Parameters* and *Fabric Parameters* from the *Configure* menu at any view. The *Configure Switch Parameters* dialog box displays.

e. Type the customer-determined preferred domain ID value, then click *OK* or *Activate*.

f. Repeat steps **d** and **e** at the second product (attached to the segmented E_Port). Use a different preferred domain ID value.

g. Set both products online. Refer to *Setting Online State* (EFCM Basic Edition) or *Setting Online State* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

10

An E_Port segmented because two products had incompatible zoning configurations. An identical zone name is recognized in the active zone set for both products, but the zones contain different members.

a. Determine the desired zone name change for one of the affected products. Zone names must conform to the following rules:

   — The name must be 64 characters or fewer in length.

   — The first character must be a letter (**a** through **z**), upper or lower case.

   — Other characters must be alphanumeric (**a** through **z** or **0** through **9**), dollar sign (**$**), hyphen (**-**), caret (**^**), or underscore (_).

b. At the EFCM Basic Edition interface or SAN management application, inspect names in the active zone set to determine the incompatible zone name, then modify the name as directed by the customer:

   — **EFCM Basic Edition -** Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.

   — **SAN management application -** Refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

11

An E_Port segmented because a build fabric protocol error was detected.

a. Disconnect the fiber-optic jumper cable from the segmented E_Port.

b. Reconnect the cable to the same port.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

12

Reset the product. Refer to *IML or Reset Switch* for instructions.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

13

An E_Port segmented because no product in the fabric is capable of becoming the principal switch.

a. Inform the customer the product will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

b. Set the product offline. Refer to *Setting Online State* (EFCM Basic Edition) or *Setting Online State* (Element Manager).

c. For the product reporting the problem:

   — **EFCM Basic Edition -** Select *Switch* and *Fabric Parameters* from the *Configure* menu at any view. The *Fabric Parameters View* displays.

   — **Element Manager -** Select *Operating Parameters* and *Fabric Parameters* from the *Configure* menu at any view. The *Configure Fabric Parameters* dialog box displays.

d. At the *Switch Priority* field, select *Principal*, *Never Principal*, or *Default*, then click *OK* or *Activate*. The switch priority value designates the fabric's principal switch, which is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

   Principal is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means the fabric element is incapable of becoming a principal switch. If all elements are set to *Principal* or *Default*, the element with the highest priority and the lowest WWN becomes the principal switch. At least one element in a multiswitch fabric must be set as *Principal* or *Default*. If all elements are set to *Never Principal*, all ISLs segment.

e. Set the product online. Refer to *Setting Online State* (EFCM Basic Edition) or *Setting Online State* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

14

An E_Port segmented (operational product) because a response (hello timeout) to a verification check indicates an attached switch is not operational.

a. Perform a data collection at the operational product and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager).

b. Go to *MAP 0000: Start MAP* and perform fault isolation for the failed switch. **Exit MAP.**

15

Event code **072** indicates a product E_Port is connected to an unsupported fabric element. Advise the customer of the problem and disconnect the ISL to the unsupported fabric element. **Exit MAP.**

16

Event code **082** is informational only and indicates a product E_Port is fenced (blocked). An application or hardware malfunction occurred (as indicated by failure symptoms or primary event codes) or the port fencing policy is too restrictive. Obtain supplementary event data as follows:

a. At the *Event Log*, examine the first five bytes (**0** through **4**) of event data.

b. Byte **0** specifies the E_Port reporting the problem. Byte **4** specifies the port fence code as listed in Table 3-15.

Table 3-15 Port Fence Codes and Actions

Byte 4	Port Fence Code	Action
01	Protocol error.	Go to step 17.
02	Link-level hot I/O.	Go to step 18.
03	Security violation.	Go to step 19.

17

An E_Port is fenced because of a protocol error. Depending on failure cause, additional information and event codes are available at the product or attached switch. Perform one of the following:

- The E_Port is segmented and accompanied by primary event code **070**. **Go to step 7.**
- The fiber-optic cable is disconnected, the cable failed or is degraded, or the port optical transceiver failed. The failure is accompanied by a primary event code indicating the failure type. Go to *MAP 0000: Start MAP* and perform fault isolation for the primary event code. **Exit MAP.**
- The E_Port is fenced because of persistent incomplete operations (ISL bouncing). Go to *MAP 0000: Start MAP* and perform fault isolation at the attached switch. **Exit MAP.**
- The E_Port is fenced because of application-layer protocol errors. Go to *MAP 0000: Start MAP* and perform fault isolation at the attached switch. **Exit MAP.**

18

An E_Port is fenced because devices connected to the attached fabric element are flooding the ISL with frames (hot I/O). These link-level problems are typically associated with legacy devices, arbitrated loop devices, or magnetic tape drives. Perform one of the following:

- Disconnect the ISL. **Exit MAP.**
- Refer to the manufacturer's documentation and perform fault isolation at the attached device or fabric element. **Exit MAP.**
- Change port fencing threshold settings to more lenient values. **Go to step 20.**

19

An E_Port is fenced because of persistent firmware-related security violations (SANtegrity binding or SANtegrity authentication failures).

a. At the EFCM Basic Edition interface, SAN management application, or Element Manager, change binding membership lists or authentication parameters as directed by the customer:

— **EFCM Basic Edition -** Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.

— **SAN management application -** Refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

— **Element Manager -** Refer to the *McDATA Sphereon 4400 Fabric Switch Element Manager User Manual* (620-000241) for instructions.

b. Unblock the port. Refer to *Blocking or Unblocking a Port* (EFCM Basic Edition) or *Blocking or Unblocking a Port* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

20

Port fencing threshold settings are too restrictive.

a. At the EFCM Basic Edition interface or SAN management application, change port fencing threshold settings to more lenient values as directed by the customer:

— **EFCM Basic Edition -** Refer to the *McDATA EFCM Basic Edition User Manual* (620-000240) for instructions.

— **SAN management application -** Refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

b. Unblock the port. Refer to *Blocking or Unblocking a Port* (EFCM Basic Edition) or *Blocking or Unblocking a Port* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

21

Event codes **140** and **142** occur only if the optional OpenTrunking feature is enabled.

- **Event code 140 -** OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeds the configured congestion threshold.
- **Event code 142 -** OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This results in downstream fabric congestion.

No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If the event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the fabric elements reporting the problem.
- Increase the ISL link speed between the fabric elements reporting the problem (from 1 Gbps to 2 or 4 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

22

Event code **150** indicates a fabric merge process failed during ISL initialization. An incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes event code **070**, and represents the reply of an adjacent fabric element in response to a zone merge frame. Obtain supplementary event data as follows:

a. At the *Event Log*, examine the first 12 bytes (**0** through **11**) of event data.

b. Bytes **0** specifies the E_Port reporting the problem. Bytes **8** through **11** specify the failure reason as listed in Table 3-16.

Table 3-16 Fabric Merge Failure Reasons and Actions

Bytes 8 - 11	Merge Failure Reason	Action
01	Invalid data length.	Go to step 23.
08	Invalid zone set format.	Go to step 23.
09	Invalid data.	Go to step 24.
0A	Cannot merge.	Go to step 24.
F0	Retry limit reached.	Go to step 23.
F1	Invalid response length.	Go to step 23.
F2	Invalid response code.	Go to step 23.

23

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Reason 01 -** An invalid data length condition caused an error in a zone merge frame.
- **Reason 08 -** An invalid zone set format caused an error in a zone merge frame.
- **Reason F0 -** A retry limit reached condition caused an error in a zone merge frame.
- **Reason F1 -** An invalid response length condition caused an error in a zone merge frame.
- **Reason F2 -** An invalid response code caused an error in a zone merge frame.

Disconnect the fiber-optic jumper cable from the E_Port reporting the problem, then reconnect the cable to the same port.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). **Exit MAP.**

24

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Reason 09 -** Invalid data caused a zone merge failure.
- **Reason 0A -** A *Cannot Merge* condition caused a zone merge failure.

Obtain supplementary error code data for event code **150**. At the *Event Log*, examine bytes **12** through **15** of event data that specify the error code. Record the error code.

Perform a data collection and contact the next level of support. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (Element Manager). Report the event code, associated failure reason, and supplementary error code. **Exit MAP.**

4

Repair Information

This chapter describes repair-related procedures for the Sphereon 4400 Fabric Switch. The procedures are performed at the switch, a browser-capable PC communicating with the product-resident Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface, or a rack-mount management server running a storage area network (SAN) management application. The chapter describes:

- *Procedural Notes* on page 4-2
- *Power On Switch* on page 4-2
- *Power Off Switch* on page 4-3
- *IML or Reset Switch* on page 4-3
- *Clean Fiber-Optic Components* on page 4-5.
- *Download Firmware or Software from the Filecenter* on page 4-6
- *Port LED Diagnostics* on page 4-8
- *Repair Procedures - EFCM Basic Edition* on page 4-10
- *Repair Procedures - SAN Management Application* on page 4-28

Procedural Notes

Observe the following procedural notes:

1. Follow all electrostatic discharge (ESD) precautions and **DANGER**, **CAUTION**, and **ATTENTION** statements.
2. Before performing a procedure, read the procedure carefully and thoroughly to familiarize yourself with the information.

Power On Switch

To power on the switch:

1. One alternating current (AC) power cord is required for each external power supply. Ensure the correct power cords are available.

DANGER

Use the supplied power cords. Ensure that the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded. (D004)

2. Plug power cords into facility power sources and AC connectors on each external power supply.
3. Connect each power supply adapter cord to a threaded output jack at the rear of the switch.
4. Twist the cord clockwise to lock and secure the connection. When the first adapter cord is connected, the switch powers on and performs power-on self-tests (POSTs).

NOTE: For high availability, plug the power cords into separate facility power circuits.

During POSTs:

— The green **PWR** LED on the switch front panel illuminates.

— The amber **ERR** LED on the switch front panel blinks momentarily while the switch is tested.

— The green LED associated with the Ethernet port blinks momentarily while the port is tested.

— The green and amber LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.

After successful POST completion, the **PWR** LED remains illuminated and all amber LEDs extinguish.

5. If a POST error occurs, go to *MAP 0000: Start MAP* to isolate the problem.

Power Off Switch

Inform the customer the switch is to be powered off. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

To power off the switch, use the following steps:

1. Set the switch offline. Refer to *Setting Online State* (EFCM Basic Edition) or *Setting Online State* (Element Manager) for instructions.
2. Twist external power supply adapter cords counterclockwise to unlock connections, then disconnect cords from threaded output jacks at the rear of the switch.

IML or Reset Switch

An initial machine load (IML) or reset is performed at the switch front panel using the **RESET** button. An IML does not cause power-on diagnostics to execute and is not disruptive to Fibre Channel traffic. An IML:

- Reloads switch firmware from FLASH memory.
- Resets the Ethernet LAN interface, causing the connection to the browser PC or management server to drop momentarily until the connection automatically recovers.

A reset is disruptive to Fibre Channel traffic and resets the:

- Microprocessor and functional logic for the control processor (CTP) card and reloads the firmware from FLASH memory.

- Ethernet LAN interface, causing the connection to the browser PC or management server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

ATTENTION ! A reset should only be performed if a CTP card failure is indicated. Do not reset a switch unless directed to do so by a procedural step or the next level of support.

IML

To IML the switch use the following steps:

1. Press and hold the **RESET** button (about three seconds) until the amber **ERR** LED blinks at twice the unit beaconing rate.
2. Release the button. During the IML, the switch-to-browser PC (or management server) Ethernet link drops momentarily.

Reset

To reset the switch use the following steps:

1. Press and hold the **RESET** button for ten seconds.
   - — After holding the button for three seconds, the amber **ERR** LED blinks at twice the unit beaconing rate.
   - — After holding the button for ten seconds, the **ERR** LED stops blinking, and all front panel LEDs illuminate.
2. Release the button to reset the switch. During the reset:
   - — The green **PWR** LED on the switch front panel illuminates.
   - — The amber **ERR** LED on the switch front panel blinks momentarily while the switch is tested.
   - — The green LED associated with the Ethernet port blinks momentarily while the port is tested.
   - — Green and amber LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.
   - — The switch-to-browser PC (or management server) Ethernet link drops momentarily.

Clean Fiber-Optic Components

Perform this procedure as directed by a service procedural step or when connecting or disconnecting fiber-optic cables from port optical transceivers.

The following tools (supplied by service personnel) are required:

- ESD grounding cable and wrist strap.
- Fiber-optic cleaning kit with:
  - — Oil-free compressed air or HFC-134a aerosol duster.
  - — Alcohol-soaked cleaning pads.

CAUTION

Wear eye protection when using an aerosol duster.

To clean fiber-optic components use the following steps:

1. Optical transceivers are ESD-sensitive. Ensure an ESD grounding cable is connected to the product chassis and your wrist.
2. Disconnect the fiber-optic cable from the optical transceiver as directed by a customer representative or service procedural step.
3. Use an aerosol duster to blow any contaminants from the component (part 1 of Figure 4-1).
   - — Hold the duster upright and keep the air nozzle approximately 50 millimeters (two inches) from the end of the component.
   - — For approximately five seconds, continuously blow compressed air or HFC-134a gas on exposed surfaces and the end-face of the component.

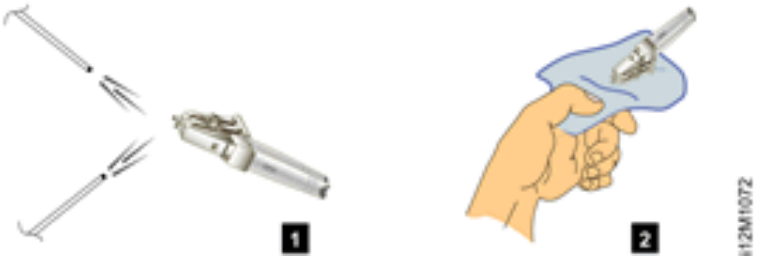


Figure 4-1 Clean Fiber-Optic Components

4. Gently wipe the end-face and other surfaces of the component with an alcohol pad (part 2 of Figure 4-1). Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for cleaned surfaces to dry.
5. Repeat steps two and three (second cleaning).
6. Repeat steps two and three (third cleaning).
7. Reconnect the fiber-optic cable to the optical transceiver.

Download Firmware or Software from the Filecenter

The firmware version shipped with the product is provided on the *System Version XX.YY.ZZ* CD-ROM. The SAN management application (software) shipped with the product is provided on the *EFC Management Applications* CD-ROM. Subsequent (upgrade) firmware and software versions are provided to customers through the McDATA Filecenter.

NOTE: When upgrading firmware or software, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the version. Such information supplements information provided in this general procedure.

Download the firmware or software version to the hard drive of a server with Internet access. This server can be the rack-mount management server or PC communicating with the EFCM Basic Edition interface.

To download a firmware or software version use the following steps:

1. Open the McDATA home page (**http://mcdata.com**). Select *File Center* from the *Support* menu. The Filecenter home page opens (Figure 4-2).

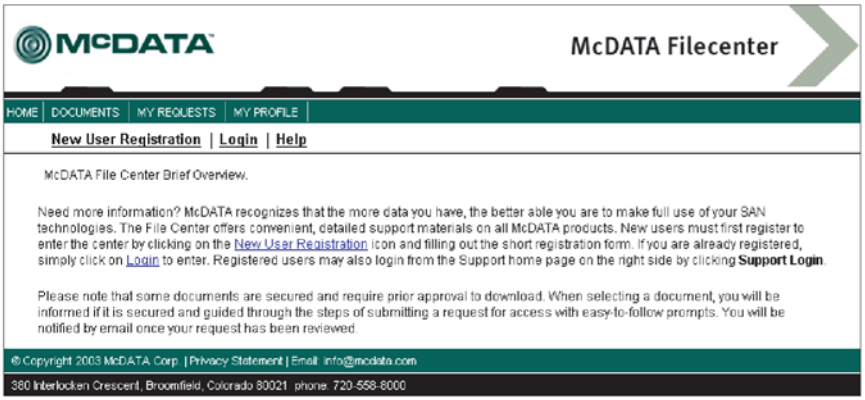

McDATA
McDATA Filecenter
HOME
DOCUMENTS
MY REQUESTS
MY PROFILE
New User Registration | Login | Help
McDATA File Center Brief Overview.
Need more information? McDATA recognizes that the more data you have, the better able you are to make full use of your SAN technologies. The File Center offers convenient, detailed support materials on all McDATA products. New users must first register to enter the center by clicking on the New User Registration icon and filling out the short registration form. If you are already registered, simply click on Login to enter. Registered users may also login from the Support home page on the right side by clicking Support Login.
Please note that some documents are secured and require prior approval to download. When selecting a document, you will be informed if it is secured and guided through the steps of submitting a request for access with easy-to-follow prompts. You will be notified by email once your request has been reviewed.
© Copyright 2003 McDATA Corp. | Privacy Statement | Email: info@mcdata.com
380 Interlocken Crescent, Broomfield, Colorado 80021 phone: 720-558-8000
i16M2006

Figure 4-2 McDATA Filecenter Home Page

2. Select (click) *Login* at the top of the page. The *Login* page appears.
3. Type a user name and password (assigned and registered while performing *Task 24: Register with the McDATA Filecenter*) and click *Login*. The *Welcome, you have been logged in* page appears.
4. Select (click) *Documents* at the top of the page. The *Search / New Documents / By Category* page appears.
5. Select (highlight) the desired option (firmware or software) from the list box and click *Search*. The *Documents Match* page appears with a list of firmware or software available for download.
6. As the secure symbol ( ) in the *Status* column indicates, authorization to download a firmware or software version requires approval. In the *Action* column adjacent to the desired version, click *Add to Request*. The *Current Request: Not Yet Submitted* page appears.
7. Type the serial number of the product at the *Associated Serial Number* field, to which the firmware or software download applies and click *Submit Request*. The *Request Submitted* page appears and the request for approval is e-mailed to support personnel.

8. Wait approximately five minutes for a response, then select (click) *My Requests* at the top of the page. The *Request History* page appears with the approved request (indicated by an approved symbol (A) in the *Status* column).
9. In the *Action* column adjacent to the approved request for the firmware or software version, click *Download*. The *File Download* dialog box appears.
10. Click *Save*. The *Save As* dialog box appears.
11. At the *Save As* dialog box, ensure the correct directory path is specified at the *Save in* field, the correct file is specified in the *File name* field, and click *Save*.
12. A *Download* dialog box appears, showing the estimated time remaining to complete the firmware or software download process. When the process finishes, the dialog box changes to a *Download complete* dialog box.
13. Click *Close* to close the dialog box. The new firmware or software version is downloaded and saved to the server hard drive.
14. Close the Internet session.
15. If required, transfer the downloaded file from the server to the rack-mount management server or PC communicating with the EFCM Basic Edition interface. Use a diskette, CD-ROM, or other electronic means.

Port LED Diagnostics

Fibre Channel port diagnostic information is obtained by inspecting port LEDs at the product front panel or emulated port LEDs at the management interface (EFCM Basic Edition interface or SAN management application). LEDs adjacent to each port and software alert symbols indicate operational status as described in Table 4-1

.

Table 4-1 Port Operational States

Port State	Green LED	Amber LED	Alert Symbol	Description
Online	On or Blinking	Off	None	An attached device is ready to communicate, or is communicating with other devices. Green LED illuminates.

Table 4-1 Port Operational States (*continued*)

Port State	Green LED	Amber LED	Alert Symbol	Description
Offline	Off	Off	None	Port is blocked and transmitting the offline sequence (OLS) to attached device.
	Off	Off	Yellow Triangle	Port is unblocked and receiving the OLS, indicating attached device is offline.
Beaconing	Off, On, or Blinking	Blinking	Yellow Triangle	Port is beaconing. Amber LED blinks once every two seconds to enable users to locate port.
Invalid Attachment	On	Off	Yellow Triangle	Port has an invalid attachment. Reason appears as supplementary data in the *Event Log*.
Link Incident	Off	Off	Yellow Triangle	Link incident occurred. Reason appears in the *Link Incident Log*.
Link Reset	Off	Off	Yellow Triangle	Product and attached device are performing a link reset to recover the connection. Transient state that does not persist.
No Light	Off	Off	None	No signal (light) is received at product port. Normal condition when no cable is attached to port or when attached device is powered off.
Inactive	On	Off	Yellow Triangle	Port is inactive. Reason appears at *Port List View* or *Port Properties* dialog box.
Not Installed	Off	Off	None	Optical transceiver not installed in the port.
Not Operational	Off	Off	Yellow Triangle	Port is receiving the not operational sequence (NOS) from attached device.
Port Failure	Off	On	Red and Yellow Blinking Diamond	Port failed and requires service.
Segmented E_Port	On	Off	Yellow Triangle	E_Port segmented, preventing connected switches from forming a fabric. Reason appears as supplementary data in the *Event Log*.
Testing	Off	Blinking	Yellow Triangle	Port is performing an internal loopback test.
	On	Blinking	Yellow Triangle	Port is performing an external loopback test.

Repair Procedures - EFCM Basic Edition

The following procedures (performed at a PC communicating with the EFCM Basic Edition interface) are described:

- *Obtaining Log Information* on page 4-10
- *Performing Port Diagnostics* on page 4-13
- *Collecting Maintenance Data* on page 4-20
- *Setting Online State* on page 4-21
- *Blocking or Unblocking a Port* on page 4-22
- *Upgrading Firmware* on page 4-23
- *Managing Configuration Data* on page 4-25

Obtaining Log Information

The EFCM Basic Edition interface provides access to logs that contain maintenance information. Select the desired log from the *Logs* menu at any view. Logs with maintenance information are:

- Event.
- Link Incident.
- Audit
- Security
- Open Trunking Re-Route.
- Fabric.
- Embedded Port Frame.
- Syslog Configuration.

Event Log

The *Event Log* records events or errors. Entries reflect the status of the management interface and managed product. The log describes:

- **Date/Time -** Date and time the event occurred.
- **Error Code -** Three-digit code that describes the event. Event codes are listed and described in Appendix A, *Event Code Tables*.
- **Severity -** Event severity (*Informational*, *Minor*, *Major*, or *Severe*).
- **Event Data -** Supplementary information (if available) in hexadecimal format. Event data is described in Appendix A, *Event Code Tables*.

Link Incident Log

The *Link Incident Log* records Fibre Channel link incident events and causes. The log describes:

- **Date/Time -** Date and time the link incident occurred.
- **Port -** Port number reporting the link incident.
- **Link Incident Event -** Brief description of the link incident and cause, including:
  - — Implicit incident.
  - — Bit-error threshold exceeded.
  - — Loss of signal or loss of synchronization.
  - — Not-operational primitive sequence received.
  - — Primitive sequence timeout.
  - — Invalid primitive sequence received for current link state.

Refer to *MAP 0500: Port Failure or Link Incident Analysis* for corrective actions.

Audit Log

The audit log appears a history of all configuration changes applied to the switch from any source such as Element Manager, SNMP management stations, or host. The audit log provides:

- **Date/Time -** The date and time of the log entry.
- **Source -** The source of Audit Log event.
- **User ID -** Identifier of the user that issued the command. The identifier is usually an IP address.
- **Action -** The type of Audit Log event.

Security Log

The security log provides:

- **Reason -** The reason code for the security event
- **Date/Time -** The date/time when the event occurred.
- **Trigger Level -** The trigger level of the event. Possible values include: Informational, Security Change, or Error
- **Count -** A cumulative count of events within a known period.
- **Category -** The event category message with possible values may be: Successful Connection, Disconnection, Configuration Change, Authorization Failure, Authentication Failure, or Reserved.
- **Description -** Description of the event.

- **Data -** Any extra or event specific data.

Open Trunking Re-Route Log

The *Open Trunking Re-Route Log* records interswitch link (ISL) congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed product. The log describes:

- **Date/Time -** Date and time the re-route occurred.
- **Receive Port -** Target port number (decimal) receiving Fibre Channel traffic after the re-route.
- **Target Domain -** Target device domain ID (decimal) receiving Fibre Channel traffic after the re-route.
- **Old Exit Port -** Port number (decimal) transmitting Fibre Channel traffic before the re-route.
- **New Exit Port -** Port number (decimal) transmitting Fibre Channel traffic after the re-route.

Fabric Log

The *Fabric Log* records the time and nature of changes made to a multiswitch fabric. The information is useful for isolating zoning or fabric-wide problems. The log describes:

- **Count -** Cumulative count of log entries (wrapping or non-wrapping).
- **Date/Time -** Date and time the change occurred.
- **Description -** Description of the zoning or fabric change.
- **Data -** Supplementary information (if available) in text format.

NOTE: Identical entries are recorded in the wrapping and non-wrapping logs. When the non-wrapping log fills, old records are overwritten. The wrapping log preserves all records.

Embedded Port Frame Log

The *Embedded Port Frame Log* records all Fibre Channel frames transmitted through the product's embedded port, including Class F traffic, fabric logins, state change notifications, and exception frames. The information is useful for Fibre Channel frame debugging (usually performed by second-level support. The log describes:

- **Count -** Cumulative count of log entries (wrapping or non-wrapping).
- **Date/Time -** Date and time frame was transmitted through the embedded port.

- **Port # -** Fibre Channel port number (decimal) transmitting frame through the embedded port.
- **Direction -** Fibre Channel frame direction - incoming (**I**) or outgoing (**O**).
- **SOF -** Start of frame character (hexadecimal).
- **EOF -** End of frame character (hexadecimal).
- **Payload Size -** Size of frame payload in bytes.
- **Header -** 24-byte frame header (hexadecimal).
- **Payload -** First 32 bytes of frame payload (hexadecimal).

Syslog Configuration

The Syslog Configuration page enables you to configure client systems to receive logs from the product.

A remote host receives copies of the system logs (syslogs), providing a means to view logs if the product is unavailable.

The recipient clients are identified by IP address. You can specify multiple clients for receiving logs. The interface also enables you to choose which logs the product sends to its syslog recipients.

The following tasks can be performed using the Syslog Configuration:

- Enable and disable syslogs.
- Add a syslog recipient to the list.
- Edit information for a syslog recipient.
- Delete syslog recipients from the list.
- Identify which logs are sent to recipients.

Performing Port Diagnostics

Fibre Channel port diagnostic information is obtained by:

- Inspecting port properties, predictive optics monitoring (POM) data, or port transceiver technology information at the lower panel of the *Port List View*.
- Inspecting statistical information at the *Performance View*.
- Performing an internal or external loopback test.

Port List View

The EFCM Basic Edition interface provides access to port diagnostic information through the *Port List View*. To open this view, select *Port*

List from the *Product* menu at any view. As an example, the figure shows POM data in the lower panel (Figure 4-3).

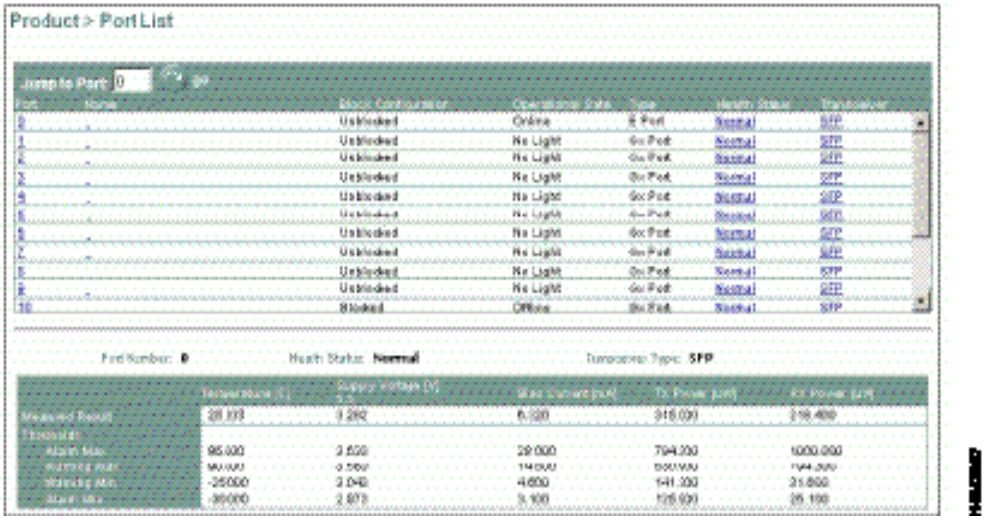


Figure 4-3 Port List View

A row of information for each port appears. Each row consists of the following columns::

Table 4-2 Port List Table

Port Property	Description
Port	The product port number.
Name	The user-defined name or description for the port.
Block Configuration	Indicates if a port is blocked or unblocked.
Operational State	Port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, or *Testing*).
Type	The type of port, including generic mixed port (*GX_Port*), fabric mixed port (*FX_Port*), generic port (*G_Port*), fabric port (*F_Port*), or expansion port (*E_Port*).
Health Status	The condition of the installed optical transceiver (*Normal*, *Warning*, *Alarm*, or *No Info*).
Transceiver	Installed transceiver type (*SFP*, *XFP*, or *Unknown*).

Inspect Port Properties

At the *Port List View,* click a physical port number listed in the *Port* column. Physical properties for the selected port appear in the lower panel of the view:

Table 4-3 Inspect Port Properties Table

Port Property	Description
Port Number	The product's port number.
Port Name	The user-defined name or description for the port.
Port Type	The user-defined port type (*GX_Port*, *FX_Port*, *G_Port*, *F_Port*, or *E_Port*).
Operating Speed	The port operating speed (*Not Established*, *1 Gbps*, *2 Gbps*, or *4 Gbps*)
Fibre Channel Address	The Port FC address identifier. Port FC address if the port was swapped.
Port WWN	The Fibre Channel world wide name (WWN) of the port.
Attached Port WWN	Fibre Channel WWN of the device attached to the port.
Block Configuration	The user-configured state for the port (*Blocked* or *Unblocked*).
Block Reason	The reason for blocking the port.
Beaconing	The user-specified for the port (*On* or *Off*).
FAN Configuration	User-configured state for fabric address notification (FAN) configuration (*Enabled* or *Disabled*).
RX BB Credit	The number of receive BB credits available for the port.
Operational State	The port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, *Disabled*, or *Testing*).
Reason	A summary appears describing the reason if the port state is *Segmented E_Port*, *Invalid Attachment*, or *Inactive*. For any other port state, the reason is *N/A*.

Inspect POM Data

At the *Port List View*, click the entry for a port in the *Health Status* column. POM data for the selected port appears in the lower panel of the view (Figure 4-3):

Table 4-4 POM Data Table

Port Property	Description
Port Number	The product's port number.
Health Status	The condition of the installed optical transceiver (*Normal*, *Warning*, *Alarm*, or *No Info*).
Transceiver Type	The installed transceiver type (*SFP*, *XFP*, or *Unknown*).

If the port has a digital diagnostics (DD) enabled optical transceiver installed, product firmware appears a table of reported temperature, voltage, current, transceiver power, and receiver power. Optical transceivers also provide vendor-specific threshold values for these parameters.

Inspect Port Transceiver Technology

At the *Port List View*, click the entry for a port in the *Transceiver* column. Port transceiver technology information for the selected port appears in the lower panel of the view:

Table 4-5 Inspect Port Transceiver Technology Table

Port Property	Description
Port Number	The product's port number.
Identifier	The installed transceiver type (*SFP*, *XFP*, or *Unknown*).
Connector type	The type of port connector (*LC*, *MT_RJ*, *MU*, *Unknown*, or *Internal Port*).
Transceiver	The type of port transceiver (*Shortwave Laser*, *Longwave Laser*, *Long Distance Laser*, *Unknown*, or *None*).
Distance Capability	The port transmission distance (*Short*, *Intermediate*, *Long*, *Very Long*, or *Unknown*).
Media	The type of optical cable used (*Singlemode*, *multimode 50-micron*, *multimode 62.5-micron*, or *Unknown*).
Speed	The operating speed (*Not Established*, *1 Gbps*, *2 Gbps*, or *4 Gbps*).

Performance View

The EFCM Basic Edition interface provides access to port statistics information through the *Performance View*.

- To open this view, select *Performance* from the *Product* menu (*Product>Performance*). The following statistical information appears:

Table 4-6 Performance View Table

Statistics	Description
Traffic Statistics	Port transmit and receive values for frames Four-byte words transmit and receive value for frames Offline sequences transmit and receive value for frames Link resets and link utilization percentage. Time spent using no transmission buffer-to-buffer credit (BB_Credit)
Error Statistics	Number of: Link failures Synchronization and signal losses Discarded frames Invalid transmission words Primitive sequence errors Cyclic redundancy check (CRC) errors Delimiter errors Address identification errors Short frames.
Class 2 Statistics	Number of: 4-byte words transmitted and received Class 2 frames transmitted, received, busied, or rejected.
Class 3 Statistics	Number of: 4-byte words transmitted and received Class 3 frames transmitted, received, or discarded.
Open Trunking Statistics	These statistics include the number of traffic flows rerouted to or from an ISL due to congestion.

Internal Loopback Test

An internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of an optical transceiver, but does not check fiber-optic components of the installed transceiver. Operation of the attached device is disrupted during the test.

Inform the customer a disruptive internal loopback test is to be performed. Ensure the system administrator quiesces Fibre Channel frame traffic through the por and sets the attached device offline.

NOTE: A small form factor pluggable (SFP) optical transceiver must be installed in the port during the test. A device can remain connected during the test.

To perform the test use the following steps:

1. Select *Diagnostics* from the *Maintenance* menu (*Maintenance>Ports>Diagnostics*). The *Diagnostics View* appears (Figure 4-4).

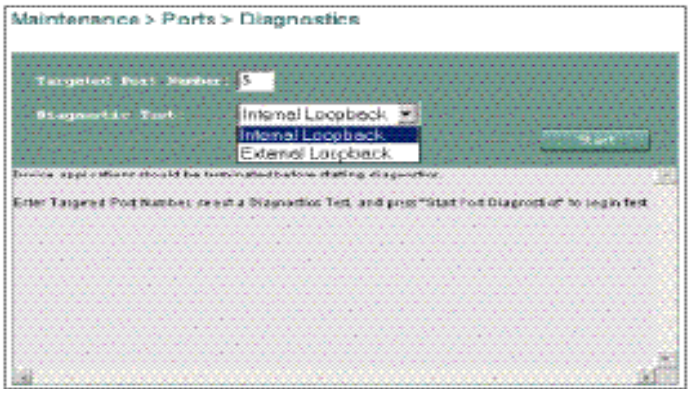


Figure 4-4 Diagnostics View

2. Type the port number to be tested in the *Targeted Port Number* field.
3. Select the *Internal Loopback* option, at the *Diagnostic Test* list box.
4. Click *Start*. The test begins and:
   a. The *Diagnostics View* changes to a *Diagnostics - Executing View*.
   b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

NOTE: Click *Stop* at any time to abort the loopback test.

When the test completes, the *Diagnostics - Executing View* reverts to the *Diagnostics View*. Test results appear as **Passed**, **Failed,** or **Test Incomplete** in the message area of the view.

5. Reset the tested port:
   a. Select *Ports* and *Reset* from the *Maintenance* menu at any view. The *Reset View* appears.
   b. For the tested port, click (enable) the check box in the *Reset* column. A check mark in the box indicates the port reset option is enabled.
   c. Click *OK*. The port resets.
6. Inform the customer that the test is complete and the attached device can be set online.

External Loopback Test

An external loopback test checks all port circuitry, including fiber-optic components of the installed optical transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a multimode loopback plug must be inserted in the port.

Inform the customer a disruptive external loopback test is to be performed and the attached device must be disconnected.

To perform the test, use the following steps:

1. Disconnect the fiber-optic jumper cable from the port to be tested.
2. Insert a multimode loopback plug into the port receptacle.
3. Select *Ports* and *Diagnostics* from the *Maintenance* menu (*Maintenance>Diagnostics*). The *Diagnostics View* appears (Figure 4-4).
4. Type the port number to be tested in the *Targeted Port Number* field.
5. Select the *External Loopback* option at the *Diagnostic Test* list box .
6. Click *Start*. The test begins and:
   a. The *Diagnostics View* changes to a *Diagnostics -Executing View*.
   b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

NOTE: Click *Stop* at any time to abort the loopback test.

When the test completes, the *Diagnostics - Executing View* reverts to the *Diagnostics View*. Test results appear as **Passed**, **Failed,** or **Test Incomplete** in the message area of the view.

7. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port (disconnected in step 1).
8. Reset the tested port:
   a. Select *Ports* and *Reset* from the *Maintenance* menu at any view. The *Reset View* appears.
   b. For the tested port, click (enable) the check box in the *Reset* column. A check mark in the box indicates the port reset option is enabled.
   c. Click *OK*. The port resets.
9. Inform the customer that the test is complete and the device can be reconnected and set online.

Collecting Maintenance Data

When firmware detects a critical error, the product automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the CTP card. Perform this procedure after a firmware fault or FRU failure to capture data for analysis by support personnel. Maintenance data includes the dump file and engineering logs.

NOTE: An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through a product feature enablement (PFE) key, a memory dump file (that may include classified Fibre Channel frames) is not included as part of the data collection procedure.

To collect maintenance data use the following steps:

1. Select *System Files* from the *Maintenance* menu (*Maintenance>System Files*). The *System Files View* appears (Figure 4-5).

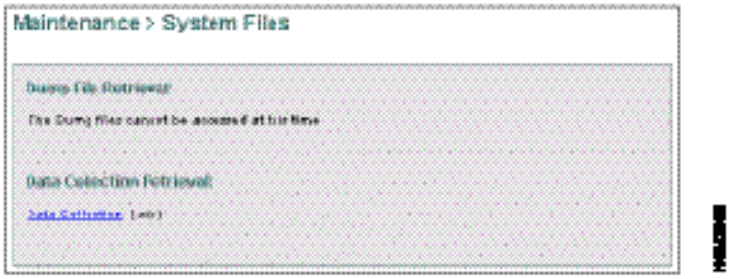


Figure 4-5 System Files View

2. Right-click the *Data Collection* link to open a list of menu options. Select the *Save Target As* menu option. The *Save As* dialog box appears.
3. Insert a blank diskette in the floppy drive of the PC communicating with the EFCM Basic Edition interface.
4. At the *Save As* dialog box, select the floppy drive (**A:**) from the *Save in* drop-down menu, type a descriptive name for the zipped (**.zip**) dump file in the *File name* field, and click *Save*.
5. A *Download* dialog box appears, showing the estimated time remaining to complete the download process. When finished, the dialog box changes to a *Download complete* dialog box.
6. Click *Close* to close the dialog box.
7. Remove the diskette with the newly-collected maintenance data from the PC floppy drive. Return the diskette with the failed FRU to support personnel for failure analysis.

Setting Online State

This section describes procedures to set the product online or offline. Operational states are:

- **Online -** When the product is set online, an attached device can log in if the port is not blocked. Attached devices in the same zone can communicate with each other.
- **Offline -** When the product is set offline, all ports are set offline and operation of attached Fibre Channel devices is disrupted. The product transmits the OLS to attached devices, and the devices cannot log in.

NOTE: Do not set the product offline unless directed to do so by a procedural step or the next level of support.

To set the product online or offline use the following steps:

1. Select *Switch* from the *Maintenance* menu (*Maintenance>Switch*). The *Switch View* appears (Figure 4-6).

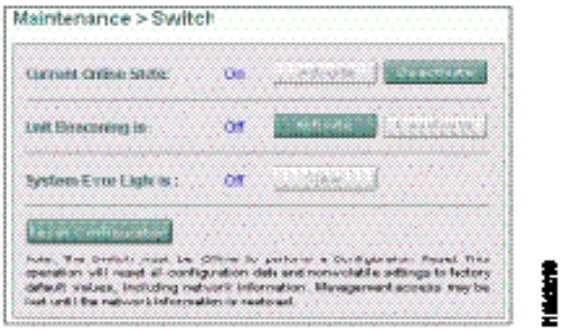


Figure 4-6 Switch View

2. Perform one of the following:
   - If the product is offline, click the *Activate* button adjacent to the *Current Online State:* field. The product comes online.
   - If the product is online, click the *Deactivate* button adjacent to the *Current Online State:* field. The product goes offline.

Blocking or Unblocking a Port

This section describes procedures to block or unblock a Fibre Channel port. Blocking a port prevents an attached device or fabric element from communicating. A blocked port continuously transmits the OLS. To block or unblock a port use the following steps:

1. Select *Ports* and *Basic Info* from the *Configure* menu (*Configure>Ports>Basic Info*). The *Basic Information View* appears (Figure 4-7).

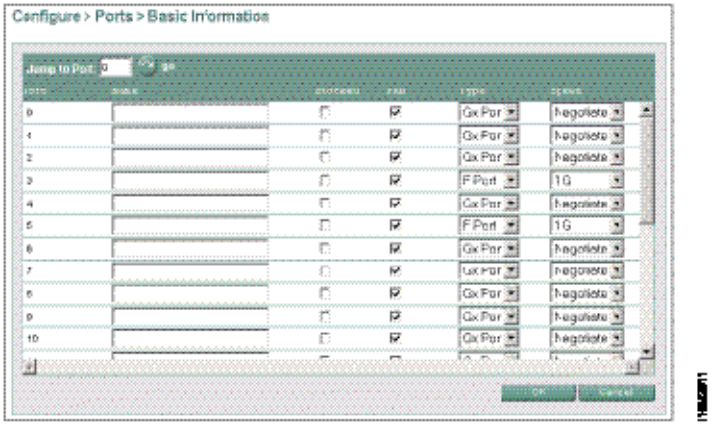


Figure 4-7 Basic Information View

2. Perform one of the following:
   - — Click the check box for the selected port in the *Blocked* column to block the port (default is unblocked). A check mark in the box indicates the port is blocked.
   - — Click the check box for the selected port in the *Blocked* column to remove the check mark and unblock the port. A blank box indicates the port is unblocked.
3. Click *OK* to save and activate changes.

Upgrading Firmware

Firmware is the product operating code stored in FLASH memory on the CTP card. Multiple firmware versions can be stored on a PC hard drive and made available for download through the EFCM Basic Edition interface. Perform the following firmware upgrade tasks at the EFCM Basic Edition interface:

- Determine the active firmware version.
- Download a firmware version.

Determine Firmware Version

To determine a firmware version, select *Hardware* from the *Product* menu (*Product >Hardware*). The *Hardware View* appears. At the bottom

of the page, record the firmware version listed in the *Firmware Level* field.

Download Firmware Version

Ensure that the desired firmware version is obtained from the Filecenter and resident on the hard drive of the PC communicating with the EFCM Basic Edition interface. Refer to *Download Firmware or Software from the Filecenter* for instructions.

NOTE: When upgrading firmware, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the version. Such information supplements information provided in this general procedure.

To download a firmware version use the following steps:

1. Select *Firmware Upgrade* from the *Maintenance* menu(*Maintenance>Firmware Upgrade*). The *Firmware Upgrade View* appears (Figure 4-8).

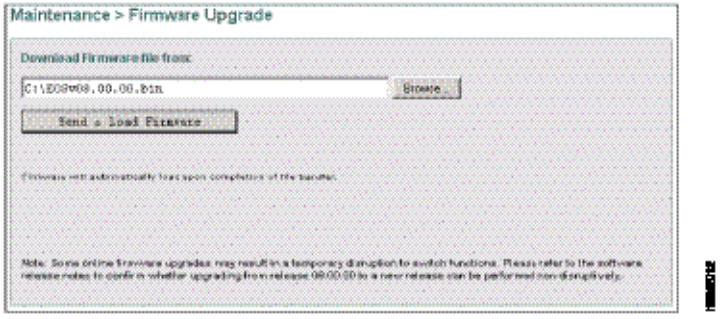


Figure 4-8 Firmware Upgrade View

2. At the *Download Firmware file from* field, select the desired file from the PC hard drive using the *Browse* button or type the desired filename.
3. Click *Send and Load Firmware*. A message box appears, indicating any browser operation will terminate the firmware download.

4. Click *OK* to download firmware. The process takes several minutes to complete, during which the browser is unavailable. When the process completes, the message **Firmware successfully received and verified. Your browser connection will be unavailable until unit restart is complete.** appears.

   After verification, the switch performs an initial program load (IPL) that takes approximately 30 seconds to complete. During the IPL, the browser-to-switch Internet connection drops momentarily and the EFCM Basic Edition session is lost.

5. After the switch IPL and EFCM Basic Edition session logout, the message **Firmware upgrade complete. Click here to login.** appears.
6. Click **here** to login and start a new EFCM Basic Edition session. The *Enter Network Password* dialog box appears.
7. Type the default user name and password.

   NOTE: The default user name is **Administrator** and the default password is **password.** Both are case-sensitive.

8. Click *OK*. The EFCM Basic Edition interface opens with the *Hardware View* panel displayed.

Managing Configuration Data

The EFCM Basic Edition interface provides options to:

- Back up and restore the configuration file stored in nonvolatile random-access memory (NV-RAM) on the switch CTP card.
- Reset the configuration file to factory default values.

The switch must be set offline prior to restoring or resetting the configuration file.

Back Up Configuration

To back up the switch configuration file to the PC communicating with the EFCM Basic Edition interface:

1. Select *Backup Configuration* from the *Maintenance* menu (*Maintenance>Backup Configuration*). The *Backup Configuration View* appears (Figure 4-9).

Figure 4-9 Backup Configuration View

2. Right-click the *Configuration file* link to open a list of menu options. Select the *Save Target As* menu option. The *Save As* dialog box appears.
3. Select the hard drive (**C:**) from the *Save in* drop-down menu at the *Save As* dialog box, type a descriptive name for the extensible markup language (**.xml**) configuration file in the *File name* field, and click *Save*.
4. A *Download* dialog box appears, showing the estimated time remaining to complete the backup process. When finished, the dialog box changes to a *Download complete* dialog box.
5. Click *Close* to close the dialog box.

Restore Configuration

To restore the switch configuration file from the PC communicating with the EFCM Basic Edition interface:

Inform the customer the switch is to be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

1. Set the switch offline. For instructions, refer to *Setting Online State*.
2. Select *Restore Configuration* from the *Maintenance* menu (*Maintenance>Restore Configuration*). The *Restore Configuration View* appears (Figure 4-10).

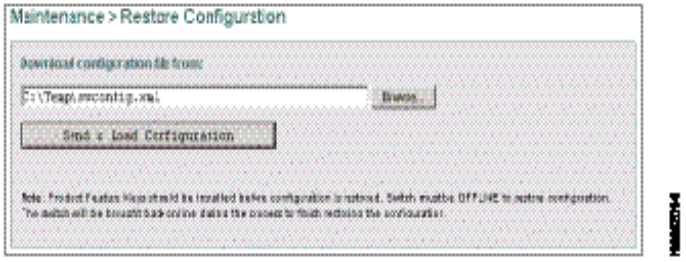


Figure 4-10 Restore Configuration View

3. Select the desired file from the PC hard drive at the *Download Configuration file from* field, using the *Browse* button or type the desired filename.
4. Click *Send and Load Configuration*. A message box appears, indicating any browser operation will terminate the configuration download.
5. Click *OK* to download the configuration. The process takes several minutes to complete, during which the browser is unavailable. When the process completes, the message **Configuration restored successfully.** appears.

Reset Configuration Data

When configuration data is reset to factory default values, the switch defaults to the factory-set (Internet Protocol) IP address and all optional features are disabled. To reset configuration data to factory default settings:

Inform the customer the switch is to be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.

1. Set the switch offline. For instructions, refer to *Setting Online State*.
2. Select *Switch* from the *Maintenance* menu (*Maintenance>Switch*). The *Switch View* appears. (Figure 4-6).
3. Click *Reset Configuration*. A dialog box with the message **Are you sure that you want to reset the configuration?** appears.
4. Click *OK* to reset the configuration.
5. The switch IP address resets to the default address of **10.1.1.10**.

— If the configured IP address (prior to reset) was the same as the default address, the browser-to-switch Internet connection is not affected and the procedure is complete.

— If the configured IP address (prior to reset) was not the same as the default address, the browser-to-switch Internet connection drops and the EFCM Basic Edition session is lost. Continue to the next step.

6. To change the switch IP address and restart the EFCM Basic Edition interface, refer to *Configure Network Information*. To restart the EFCM Basic Edition interface using the default IP address of **10.1.1.10**:

   a. Enter the default IP address of **10.1.1.10** at the browser, as the Internet URL. The *Enter Network Password* dialog box appears.

   b. Type the default user name and password.

   NOTE: The default user name is **Administrator** and the default password is **password.** The user name and password are case-sensitive.

   c. Click *OK*. The EFCM Basic Edition interface opens and the procedure is complete.

Repair Procedures - SAN Management Application

The following procedures (performed at a rack-mount management server running a SAN management application) are described. SAN management applications include EFCM 8.7 (or later).

- *Obtaining Fabric Log Information* on page 4-29
- *Obtaining Switch Log Information* on page 4-30
- *Performing Port Diagnostics* on page 4-35
- *Collecting Maintenance Data* on page 4-45
- *Setting Online State* on page 4-46
- *Blocking or Unblocking a Port* on page 4-47
- *Upgrading Firmware* on page 4-48
- *Managing Configuration Data* on page 4-51
- *Installing or Upgrading Software* on page 4-55

Obtaining Fabric Log Information

The SAN management application provides access to logs that contain fabric-level maintenance information. At the application main window, select the *Logs* option from the *Monitor* menu, then click (select) the desired log option. Logs with maintenance information are:

- Event.
- Fabric.
- Product Status.

Event Log

The *Event Log* records simple network management protocol (SNMP) trap events, client-server communication errors, and other problems recorded by the SAN management application. Information provided is generally intended for use by third-level support personnel to fault isolate significant problems. The log describes:

- **Date/Time -** Date and time the event occurred.
- **Event -** Event number and brief description of the event. Include this information when reporting an event to customer support.
- **Product -** Product associated with the event and configured name or IP address associated with the instance.
- **Data -** Additional event data for fault isolation. Include this information when fault isolating a call-home problem or reporting an event to customer support.

Fabric Log

The *Fabric Log* records the time and nature of changes made to a multiswitch fabric. The information is useful for isolating zoning or fabric-wide problems. The log describes:

- **Date/Time -** Date and time the change occurred.
- **Fabric Event -** Description of the zoning or fabric change.
- **Description -** Supplementary information (if available) in text format.

Product Status Log

The *Product Status Log* records the previous and current status of a managed product, and indicates the instance of an Element Manager application that should be opened to investigate a problem. The log describes:

- **Date/Time -** Date and time the status change occurred.

- **Network Address -** IP address or configured name of the product. The address or name corresponds to the address or name displayed under the product icon at the physical map.
- **Previous Status -** Status of the product prior to the change (*Operational*, *Degraded*, *Failed*, *Out of Band Online*, or *Unknown*). An *Unknown* status indicates the SAN management application cannot communicate with the product.
- **New Status -** Status of the product after the change (*Operational*, *Degraded*, *Failed*, *Out of Band Online*, or *Unknown*).

Obtaining Switch Log Information

The Element Manager application provides access to logs that contain switch-level maintenance information. At any application view, click (select) the desired log option from the *Logs* menu. Logs with maintenance information are:

- Audit
- Event.
- Hardware.
- Link Incident.
- Port Threshold Alert.
- Security.
- Open Trunking.
- Embedded Port.
- Switch Fabric.
- Syslog Configuration.

Audit Log

The audit log displays a history of all configuration changes applied to the switch from any source such as Element Manager, SNMP management stations, or host.

- **Date/Time -** The date and time of the log entry.
- **Source -** The source of Audit Log event.
- **User ID -** Identifier of the user that issued the command. The identifier is usually an IP address.
- **Action -** The type of Audit Log event.

Event Log

The *Event Log* records events or errors. Entries reflect the status of the management interface and managed product. The log describes:

- **Date/Time -** Date and time the event occurred.
- **Event -** Three-digit code that describes the event. Event codes are listed and described in Appendix A, *Event Code Tables*.
- **Description -** Brief description of the event.
- **Severity -** Event severity (*Informational*, *Minor*, *Major*, or *Severe*).
- **FRU-Position -** Acronym representing the FRU type, followed by a number representing the FRU chassis position.
- **Event Data -** Supplementary information (if available) in hexadecimal format. Event data is described in Appendix A, *Event Code Tables*.

Hardware Log

The *Hardware Log* records a history of FRU removals and replacements (insertions) for the switch. The log describes:

- **Date/Time -** Date and time the FRU was inserted or removed.
- **FRU -** Acronym representing the FRU type.
- **Position -** Number representing the FRU chassis position. The chassis (slot) position for a nonredundant CTP card is **0**. Chassis slots for redundant power supplies are **0** and **1**.
- **Action -** Action performed (*Inserted* or *Removed*).
- **Part Number -** Part number of the inserted or removed FRU.
- **Serial Number -** Serial number of the inserted or removed FRU.

Link Incident Log

The *Link Incident Log* records Fibre Channel link incident events and causes. The log describes:

- **Date/Time -** Date and time the link incident occurred.
- **Port -** Port number reporting the link incident.
- **Link Incident Event -** Brief description of the link incident and cause, including:
  - — Implicit incident.
  - — Bit-error threshold exceeded.
  - — Loss of signal or loss of synchronization.
  - — Not-operational primitive sequence received.

— Primitive sequence timeout.

— Invalid primitive sequence received for current link state.

Refer to *MAP 0500: Port Failure or Link Incident Analysis* for corrective actions.

Port Threshold Alert Log

The *Port Threshold Alert Log* records a history of threshold alert notifications. The log describes:

- **Date/Time -** Date and time the alert occurred.
- **Name -** Alert name as configured through the *Configure Threshold Alerts* dialog box.
- **Port -** Port number where the alert occurred.
- **Type -** Alert type: transmit (*Tx*) or receive (*Rx*).
- **Utilization % -** Percent of traffic capacity used and the threshold value configured through the *Configure Threshold Alerts* dialog box. A value of 25 means an alert occurs when throughput reaches 25% of port capacity.
- **Interval -** Time interval during which throughput is measured and an alert can generate. Set through the *Configure Threshold Alerts* dialog box.

Security Log

The security log displays the following security information:

- **Severity -** The severity level of the event (informational, warning, or fatal).
- **User -** The user associated with the event.
- **Reason -** The reason code for the event or conditions that caused the failure.
- **Description -** The security event category. The information also includes the description and details of the event and the IP address of the product.
- **Date/Time -** The date and time that the event occurred. The format is yyyy/mm/dd hh:mm:ss:tt. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Count -** The number of times that the same event occurs.
- **Category -** The category.
- **IP -** The IP address.

- **Role -** The role of the user.
- **Interface -** The interface.

Open Trunking Log

The *Open Trunking Log* records ISL congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed product. The log describes:

- **Date/Time -** Date and time the re-route occurred.
- **Receive Port -** Target port number (decimal) receiving Fibre Channel traffic after the re-route.
- **Target Domain -** Target device domain ID (decimal) receiving Fibre Channel traffic after the re-route.
- **Old Exit Port -** Port number (decimal) transmitting Fibre Channel traffic before the re-route.
- **New Exit Port -** Port number (decimal) transmitting Fibre Channel traffic after the re-route.

Embedded Port Log

The *Embedded Port Log* records all Fibre Channel frames transmitted through the product's embedded port, including Class F traffic, fabric logins, state change notifications, and exception frames. The information is useful for Fibre Channel frame debugging (usually performed by second-level support). The log describes:

- **Date/Time -** Date and time frame was transmitted through the embedded port.
- **Port -** Fibre Channel port number (decimal) transmitting frame through the embedded port.
- **Direction -** Fibre Channel frame direction (*In* or *Out*).
- **Frame Header -** 24-byte frame header (hexadecimal).
- **Length -** Size of frame payload in bytes.
- **Payload -** First 32 bytes of frame payload (hexadecimal).
- **SOF -** Start of frame character (hexadecimal).
- **EOF -** End of frame character (hexadecimal).

NOTE: Identical entries are recorded in the wrapping and non-wrapping logs. When the non-wrapping log fills, old records are overwritten. The wrapping log preserves all records.

Switch Fabric Log

The *Switch Fabric Log* records the time and nature of changes made to a multiswitch fabric that affect this product. The log describes:

- **Date/Time -** Date and time the change occurred. Timing granularity is provided to one hundredth of a second.
- **Description -** Description of the zoning or fabric change.
- **Event Data -** Supplementary event data that provides additional information that varies according to the even logged.
- **Ports (RSCN only) -** List of product ports affected by registered state change notifications (RSCNs) related to the event.

NOTE: Identical entries are recorded in the wrapping and non-wrapping logs. When the non-wrapping log fills, old records are overwritten. The wrapping log preserves all records.

Syslog Configuration

The Syslog Configuration page enables you to configure client systems to receive logs from the product.

A remote host receives copies of the system logs (syslogs), providing a means to view logs if the product is unavailable.

The recipient clients are identified by IP address. You can specify multiple clients for receiving logs. The interface also enables you to choose which logs the product sends to its syslog recipients.

The following tasks can be performed using the Syslog Configuration:

- Enable and disable syslogs.
- Add a syslog recipient to the list.
- Edit information for a syslog recipient,.
- Delete syslog recipients from the list.
- Identify which logs are sent to recipients.

Performing Port Diagnostics

Fibre Channel port diagnostic information is obtained by:

- Inspecting properties at the *Port List View*.
- Inspecting statistical information at the *Performance View*.
- Inspecting parameters at the *Port Properties* dialog box.
- Inspecting parameters at the *Port Technology* dialog box.
- Performing an internal or external loopback test.
- Swapping ports.

Port List View

The Element Manager application provides access to port diagnostic information through the *Port List View*. To open this view, click the *Port List* tab at any view (Figure 4-11). A row of information for each port appears. Each row consists of the following columns:

- **Port # -** Product port number.
- **FC Address -** Logical port address (hexadecimal format).
- **Name -** User-defined name or description for the port.

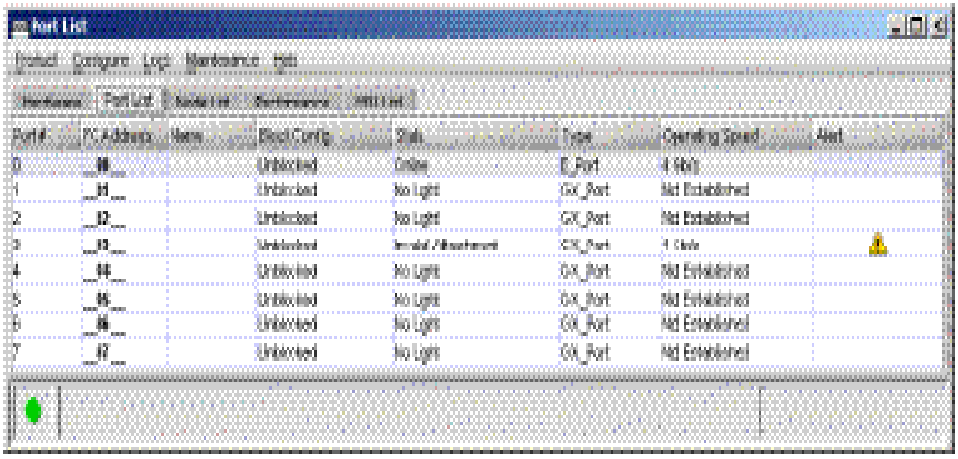


Figure 4-11 Port List View

- **Block Config -** Indicates if a port is blocked or unblocked.
- **State -** Port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, or *Testing*).

- **Type -** Port type (*GX_Port*, *FX_Port*, *G_Port*, *F_Port*, or *E_Port*).
- **Operating Speed -** Operating speed (*Not Established*, *1 Gbps*, *2 Gbps*, or *4 Gbps*).
- **Alert -** If link incident (LIN) alerts are configured, a yellow triangle appears in the column when a link incident occurs. A yellow triangle also appears if beaconing is enabled. A red and yellow diamond appears if the port fails.

Performance View

The Element Manager application provides access to port statistics information through the *Performance View*. To open this view, click the *Performance* tab at any other view.

Bar graphs at the top of the view display instantaneous transmit or receive activity level for each port. The relative value displayed is the greater of the transmit or receive activity. Each graph has 20 green-bar level indicators corresponding to 5% of maximum port throughput. If any activity is detected, at least one green bar appears. A red indicator on each bar graph (high-water mark) remains at the highest level reached since the port was set online. In addition, the following statistical information appears:

Table 4-7 Statistical Information in Performance View

Statistics Class	Description
Class 2	Number of • 4-byte words transmitted and received • Class 2 frames transmitted, received, busied or rejected
Class 3	Number of • 4-byte words transmitted and received • Class 3 frames transmitted, received, busied or rejected
Error	Number of: • Link Failures • Synchronization and signal losses • Discarded frames • Invalid transmission words • CRC • Delimiter • Address identification errors • Short frames

Table 4-7 Statistical Information in Performance View

Operational	Number of • Offline Sequences • Link resets transmitted and received
Traffic	• Port transmit and receive value for frames • Four byte words received and transmitted • Link utilization in percentage • Number of traffic flows rerouted to or from an ISL due to congestion

Port Properties Dialog Box

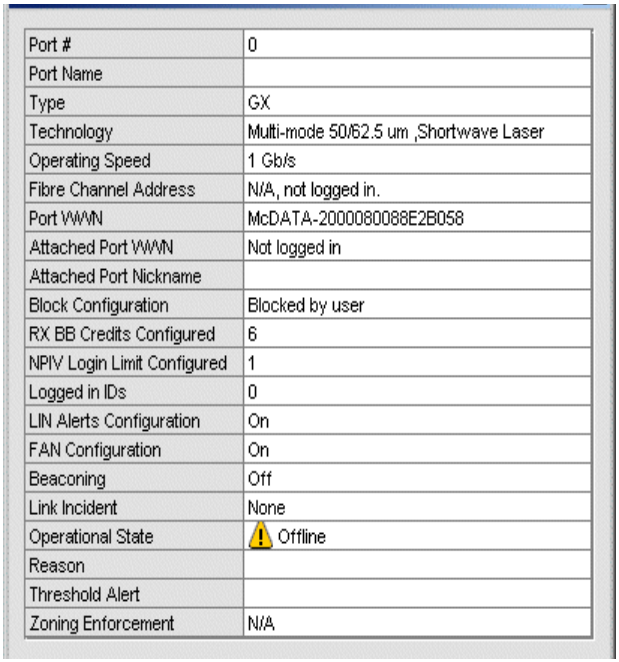
To open the *Port Properties* dialog box (Figure 4-12), double-click a port graphic at the *Hardware View* or a port row at the *Port List View*. The dialog box provides the following information::

Table 4-8 Port Properties Table

Port Property	Description
Port Number	The product's port number.
Port Name	The user-defined name or description for the port.
Type	The port type (*E_Port, F_Port, or G_Port).*
Technology	The type of port transceiver and optical cable installed.
Operating Speed	The operating speed of the port (*Not Established, 2 Gbps, or 10 Gbps*).
Fibre Channel Address	The logical port address (hexadecimal format). Not applicable for E_Ports.
Port WWN	The Fibre Channel WWN of the port.
Attached Port WWN	The Fibre Channel WWN of the device attached to the port.
Attached Port Nickname	The alternate name for the node logged into the port.
Block Configuration	A user-configured state for the port (*Blocked* or *Unblocked*).
Rx BB_Credits Configured	The user-defined number of receive BB_Credits allocated to the port.
NPIV Login Limit Configured	The user-defined maximum number of virtual addresses assigned to the physical port when N_Port ID virtualization (NPIV) enabled.
Logged in IDs	The number of virtual addresses logged in to the physical port.
LIN Alerts Configuration	A user-specified state for the port (*On* or *Off*).
FAN Configuration	A user-configured state for FAN configuration (*Enabled* or *Disabled*).

Table 4-8 Port Properties Table

Port Property	Description
Beaconing	User-specified for the port (*On* or *Off*). When beaconing is enabled, a yellow triangle appears adjacent to the status field.
Link Incident	If no link incidents are recorded, ***None*** appears in the status field. If a link incident is recorded, a summary appears describing the incident, and a yellow triangle appears adjacent to the status field.
Operational State	The state of the port (*Online*, *Offline*, *Beaconing*, *Invalid Attachment*, *Link Incident*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, or *Testing*). A yellow triangle appears adjacent to the status field if the port is in a non-standard state that requires attention. A red and yellow diamond appears adjacent to the status field if the port fails.
Reason	A summary appears describing the reason if the port state is *Segmented E_Port*, *Invalid Attachment*, or *Inactive*. For any other port state, the reason field is blank or *N/A*.
Threshold Alert	If a threshold alert exists for the port, an alert indicator (yellow triangle) and the configured name for the alert appear.
Zoning Enforcement	The zoning policy enforced (*Hard Zoning*, *Soft Zoning*, or *N/A*).



Port #	0
Port Name	
Type	GX
Technology	Multi-mode 50/62.5 um ,Shortwave Laser
Operating Speed	1 Gb/s
Fibre Channel Address	N/A, not logged in.
Port WWN	McDATA-2000080088E2B058
Attached Port WWN	Not logged in
Attached Port Nickname	
Block Configuration	Blocked by user
RX BB Credits Configured	6
NPIV Login Limit Configured	1
Logged in IDs	0
LIN Alerts Configuration	On
FAN Configuration	On
Beaconing	Off
Link Incident	None
Operational State	Offline
Reason	
Threshold Alert	
Zoning Enforcement	N/A

Figure 4-12 Port Properties Dialog Box

Port Technology Dialog Box

To view *Port Technology* (Figure 4-13), right-click a port graphic at the *Hardware View* or a port row at the *Port List View*, then select *Port Optics* from the pop-up menu. The *Port Optics* dialog box appears the *Port Technology* and *Extended Information*:

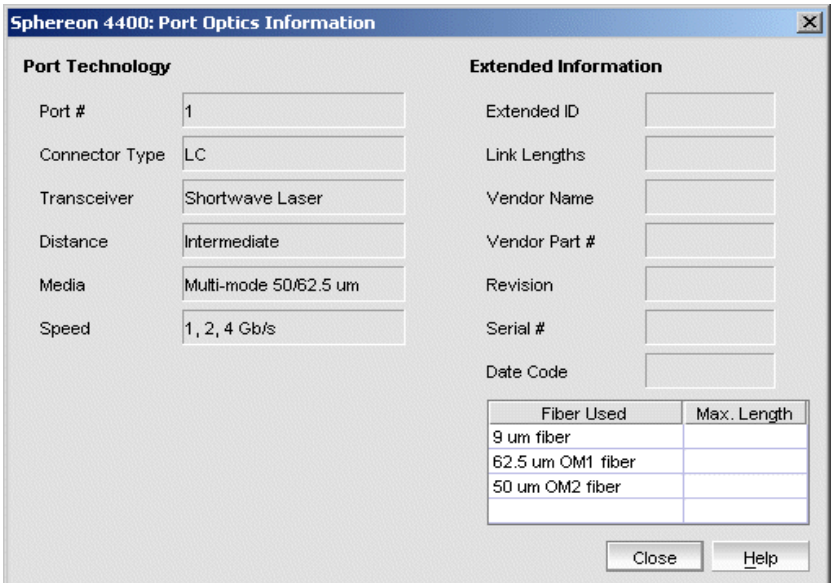


Figure 4-13 Port Technology Dialog Box

The dialog box provides the following information:

Table 4-9 Port Technology Table

Port Property	Description
Port Number	The director's port number.
Connector type	Type of port connector (*LC*, *Unknown*, or *Internal Port*).
Transceiver	Type of port transceiver (*Shortwave Laser*, *Longwave Laser*, *Long Distance Laser*, *Unknown*, or *None*).
Distance	Port transmission distance (*<=50m*, *50M - 2k*, 2k - 10k, 10k=>).
Media	Type of optical cable used (*Singlemode*, *multimode 50-micron*, *multimode 62.5-micron*, or *Unknown*).
Speed	Operating speed (*Not Established, 2 Gbps, or 10 Gbps*).
Extended Information	
Extended ID	The Extended ID
Vendor Name	The vendor manufacturing the G bic.

Table 4-9 Port Technology Table

Port Property	Description
Vendor Part #	The vendor part number.
Revision	The revision number.
Serial #	The serial number.
Date Code	The date.
Fiber used and Maximum length	Shows link lengths that are possible based on the fiber type installed. Fields are blank if data is not available.

Internal Loopback Test

An internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of an optical transceiver, but does not check fiber-optic components of the installed transceiver. Operation of the attached device is disrupted during the test. To perform the test:

Notify the customer a disruptive internal loopback test is to be performed. Ensure the system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.

NOTE: A small form factor pluggable (SFP) optical transceiver must be installed in the port during the test. A device can remain connected during the test.

1. Select *Port Diagnostics* from the *Maintenance* menu (*Maintenance>Port Diagnostics*). The *Port Diagnostics* dialog box appears (Figure 4-14).
2. Type the port number to be tested or select all ports at the *Port Select* area of the dialog box.
3. Select the *Internal Loop* option at the *Diagnostics Test* list box.
4. Click *Next*. The message **Press START TEST to begin diagnostics** appears, and the *Next* button changes to a *Start Test* button.

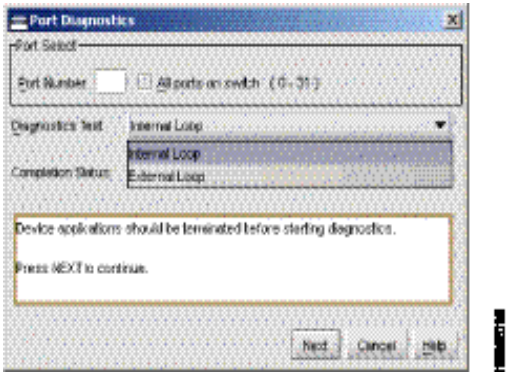


Figure 4-14 Port Diagnostics Dialog Box

5. Click *Start Test*. The test begins and:
   a. The *Start Test* button changes to a *Stop Test* button.
   b. The message **Port xx: TEST RUNNING** appears.
   c. A red progress bar (indicating percent completion) travels from left to right across the *Completion Status* field.

   When the test completes, results appear as **Port xx: Passed!** or **Port xx: Failed!** in the message area of the dialog box.
6. When finished, click *Cancel* to close the *Port Diagnostics* dialog box.
7. Reset the port:
   a. At the *Hardware View*, right-click the port graphic. A pop-up menu appears.
   b. Select *Reset Port*. A message box appears, indicating a link reset will occur.
   c. Click *OK*. The port resets.
8. Inform the customer the test is complete and the attached device can be set online.

External Loopback Test

An external loopback test checks all port circuitry, including fiber-optic components of the installed optical transceiver. To perform the test, the attached device must be quiesced and

disconnected from the port, and a multimode loopback plug must be inserted in the port. To perform the test:

Inform the customer a disruptive external loopback test is to be performed and the attached device must be disconnected.

1. Disconnect the fiber-optic jumper cable from the port to be tested.
2. Insert a multimode loopback plug into the port receptacle.
3. Select *Port Diagnostics* from the *Maintenance* menu (*Maintenance>Port Diagnostics*). The *Port Diagnostics* dialog box appears (Figure 4-14).
4. Type the port number to be tested or select all ports at the *Port Select* area of the dialog box.
5. Select the *External Loop* option at the *Diagnostics Test* list box,.
6. Click *Next*. At the *Port Diagnostics* dialog box, the message **Loopback plug(s) must be installed on ports being diagnosed** appears.
7. Ensure that the loopback plug is installed and click *Next*. The message **Press START TEST to begin diagnostics** appears, and the *Next* button changes to a *Start Test* button.
8. Click *Start Test*. The test begins and:
   a. The *Start Test* button changes to a *Stop Test* button.
   b. The message **Port xx: TEST RUNNING** appears.
   c. A red progress bar (indicating percent completion) travels from left to right across the *Completion Status* field.

   When the test completes, results appear as **Port xx: Passed!** or **Port xx: Failed!** in the message area of the dialog box.
9. When finished, click *Cancel* to close the *Port Diagnostics* dialog box.
10. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port (disconnected in step 1).
11. Reset the port:
    a. At the *Hardware View*, right-click the port graphic. A pop-up menu appears.
    b. Select *Reset Port*. A message box appears, indicating a link reset will occur.

c. Click *OK*. The port resets.

12. Inform the customer the test is complete and the device can be reconnected and set online.

Swap Ports

Failure of port circuitry behind an optical transceiver may require swapping the logical port address of the failed port to a known operational port. This ensures the port address matches information in the hardware configuration definition (HCD) of an attached host.

NOTE: This procedure swaps hexadecimal logical port addresses, not decimal port numbers.

Inform the customer a port swap is to be performed. Ensure that the system administrator quiesces Fibre Channel frame traffic through the ports, varies any attached host offline and sets any attached device offline.

To swap ports use the following steps:

1. Select *Port Swapping* from the *Maintenance* menu *(Maintenance>Port Swapping)*. The *Swap Ports* dialog box appears. (Figure 4-15).

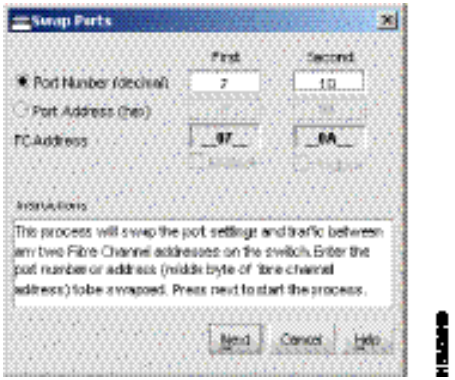

Swap Ports
First
Second
Port Number (decimal)
7
10
Port Address (hex)
FC Address
_07_
_0A_
This process will swap the port settings and traffic between any two Fibre Channel addresses on the switch. Enter the port number or address (middle byte of fibre channel address) to be swapped. Press next to start the process.
Next
Cancel
Help

Figure 4-15 Swap Ports Dialog Box

2. Select the radio button associated with the product management style and enter the decimal port numbers (open systems style) or hexadecimal port addresses (FICON style) of the ports to be swapped. The *FC Address* fields update dynamically.

3. Click *Next*. The *Instructions* section of the dialog box indicates the ports will be blocked.
4. Click *Next*. Beaconing is enabled for both ports and both ports are blocked. Swap the port fiber-optic cables as directed by the system administrator.
5. Click *Next*. The *Instructions* section of the dialog box indicates the port swap operation is complete and beaconing is disabled. Select each *Unblock* check box to unblock the ports, then click *Finish*.
6. Ensure that the system administrator varies any attached host online and sets any attached device online.
7. Back up the product configuration data. Refer to *Back Up Configuration* for instructions.

Collecting Maintenance Data

When firmware detects a critical error, the product automatically copies the contents of DRAM to a dump area in FLASH memory on the CTP card. Perform this procedure after a firmware fault or FRU failure to capture data for analysis by support personnel. Maintenance data includes the dump file and engineering logs.

NOTE: An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through a PFE key, a memory dump file (that may include classified Fibre Channel frames) is not included as part of the data collection procedure.

To collect maintenance data use the following steps:

1. Select *Data Collection* from the *Maintenance* menu (*Maintenance>Data Collection*). The *Save Data Collection* dialog box appears (Figure 4-16).

Figure 4-16 Save Data Collection Dialog Box

2. Remove the backup CD from the management server's compact disk-rewritable (CD-RW) drive and insert a blank rewritable CD.
3. Select the compact disc drive (**D:**) from the *Look in* drop-down menu at the *Save Data Collection* dialog box. Type a descriptive name for the collected maintenance data in the *File name* field, then click *Save*.
4. The *Data Collection* dialog box appears with a progress bar that shows percent completion of the data collection process. When the process reaches 100%, the *Cancel* button changes to a *Close* Button.
5. Click *Close* to close the dialog box.
6. Remove the CD with the newly-collected maintenance data from the management server's CD-RW drive. Return the CD with the failed FRU to support personnel for failure analysis.
7. To ensure that the backup application operates normally, replace the original backup CD in the management server's CD-RW drive.

Setting Online State

This section describes procedures to set the product online or offline. Operational states are:

- **Online -** When the product is set online, an attached device can log in if the port is not blocked. Attached devices in the same zone can communicate with each other.
- **Offline -** When the product is set offline, all ports are set offline and operation of attached Fibre Channel devices is disrupted. The product transmits the OLS to attached devices, and the devices cannot log in.

NOTE: Do not set the product offline unless directed to do so by a procedural step or the next level of support.

To set the product online or offline use the following steps:

1. Select *Set Online State* from the *Maintenance* menu (*Maintenance>Set Online State*). The *Set Online State* dialog box appears (Figure 4-17).

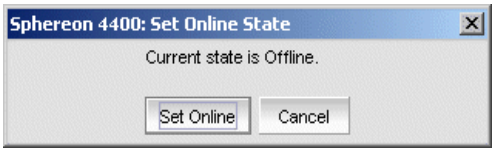


Figure 4-17 Set Online State Dialog Box

2. Perform one of the following:
   — Click *Set Online*. A warning dialog box appears the message **Performing this operation will change the current state to Online**. Click *OK*.
   — Click *Set Offline*. A warning dialog box appears the message **Performing this operation will change the current state to Offline**. Click *OK*.

Blocking or Unblocking a Port

This section describes procedures to block or unblock a Fibre Channel port. Blocking a port prevents an attached device or fabric element from communicating. A blocked port continuously transmits the OLS. To block or unblock a port:

1. Select the *Hardware* tab. The *Hardware View* for the selected switch appears.
2. Move the cursor over the port to be blocked or unblocked and right-click the mouse to open a list of menu options. Perform one of the following:
   — **To block a port:** Select the *Block Port* menu option. A *Warning* dialog box appears. Click *OK*. The dialog box closes and the following occur to indicate the port is blocked and offline:
      - At the product, the green port LED extinguishes.
      - At the *Hardware View*, the emulated green port LED extinguishes.
      - A check mark appears adjacent to the *Block Port* menu option.
   — **To unblock a port:** Select the *Block Port* menu option. Note the check mark in the box adjacent to the menu item, indicating the port is blocked. A *Warning* dialog box appears. Click *OK*. The dialog box closes and the following occur to indicate the port is unblocked and online:

- At the product, the green port LED illuminates.
- At the *Hardware View*, the emulated green port LED illuminates.
- The box adjacent to the *Block Port* menu option becomes blank.

Upgrading Firmware

Firmware is the product operating code stored in FLASH memory on the CTP card. Up to 32 firmware versions can be stored on the management server hard drive and made available for download through the Element Manager application. Perform the following firmware upgrade tasks from the management server (Element Manager application):

- Determine the active firmware version for the product.
- Add a firmware version to the management server library.
- Download a firmware version to the product.

Determine Firmware Version

To determine a switch firmware version:

1. Select *Firmware Library* from the *Maintenance* menu (*Maintenance>Firmware Library*). The *Firmware Library* dialog box appears (Figure 4-18).

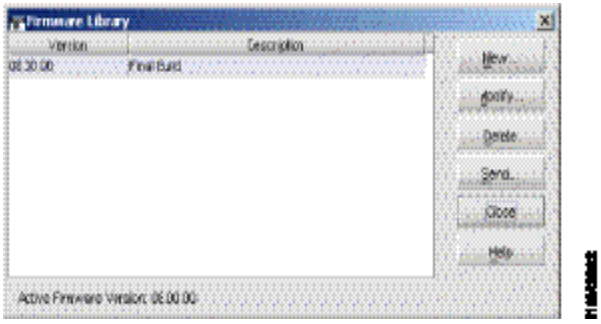


Figure 4-18 Firmware Library Dialog Box

2. The active firmware version appears at the lower left corner of the dialog box in ***XX.YY.ZZ*** format, where ***XX*** is the version level, ***YY*** is the release level, and ***ZZ*** is the patch level.

3. Click *Close* to close the dialog box.

Add Firmware Version to Management Server Library

Ensure that the desired firmware version is obtained from the Filecenter and resident on the management server hard drive. Refer to *Download Firmware or Software from the Filecenter* for instructions.

NOTE: When upgrading firmware, follow all procedural information contained in release notes or EC instructions that accompany the version. Such information supplements information provided in this general procedure.

To add a firmware version to the management server library:

1. Select *Firmware Library* from the *Maintenance* menu (*Maintenance>Firmware Library*). The *Firmware Library* dialog box appears (Figure 4-18).
2. Click *New*. The *New Firmware Version* dialog box appears.
3. Select the desired firmware version file (downloaded to the management server hard drive). Ensure the correct filename appears in the *File name* field and click *Save*. The *New Firmware Description* dialog box appears.
4. Enter a description (up to 24 characters) for the new firmware version. The description should include the installation date and text that uniquely identifies the firmware version. Click *OK*. A *File Transfer* message box appears. A progress bar travels across the message box to show percent completion.
5. Upon completion, the *File Transfer* message box converts to a *Transfer Complete* message box, indicating the new firmware version is stored on the management server hard drive. Click *Close* to close the message box.
6. The new firmware version and associated description appear in the *Firmware Library* dialog box. Click *Close* to close the dialog box.
7. To send the firmware version, refer to *Download Firmware Version*.

Download Firmware Version

To download a firmware version:

1. Before downloading firmware version ***XX.YY.ZZ***, ensure version ***XX.YY.ZZ*** or higher of the SAN management application is running on the server.

   a. Select the *About* option from the *Help* menu. The *About* dialog box appears the SAN management application version. Click *Close* to close the dialog box.

   b. If required, install the correct version of the application. For instructions, refer to *Installing or Upgrading Software*.

   As a precaution to preserve switch configuration information, perform the data collection procedure. For instructions, refer to *Collecting Maintenance Data*.

2. Select *Firmware Library* from the *Maintenance* menu. The *Firmware Library* dialog box appears (Figure 4-18).

3. Select (highlight) the firmware version to be downloaded and click *Send*. The send function verifies existence of certain switch conditions before the download process begins. If an error occurs, a message appears indicating the problem must be fixed before the firmware download. Conditions that terminate the process include:

   — A firmware version is being installed to by another user.

   — The switch-to-management server link failed or timed out.

   If a problem occurs and a corresponding message appears, go to *MAP 0000: Start MAP* to isolate the problem. If no error occurs, a *Warning* dialog box appears confirming the operation.

4. Click *Yes* to download the firmware version. The *Send Firmware* dialog box appears and the following occur during the download process:

   a. A **Writing data to FLASH** message appears at the top of the dialog box as the download begins.

   b. A **Sending Files** message appears and remains as a progress bar shows percent completion of the download. The bar progresses to 100% when the last file is transmitted to the CTP card.

   c. A **Writing data to FLASH** message appears again as the download completes.

d. The switch performs an IPL, during which an **IPLing** message appears at the *Send Firmware* dialog box. In addition, the switch-to-management server Ethernet link drops momentarily.

5. A **Send firmware complete** message appears at the *Send Firmware* dialog box.
6. Click *Close* to close the *Firmware Library* dialog box.

Managing Configuration Data

The Element Manager application provides options to:

- Back up and restore the configuration file stored in NV-RAM on the switch CTP card.
- Reset the configuration file to factory default values.

The switch must be set offline prior to restoring or resetting the configuration file.

Back Up Configuration

To back up the switch configuration file to the management server:

1. Select *Backup & Restore Configuration* from the *Maintenance* menu (*Maintenance>Backup&Restore Configuration*). The *Backup and Restore Configuration* dialog box appearsappears (Figure 4-19).

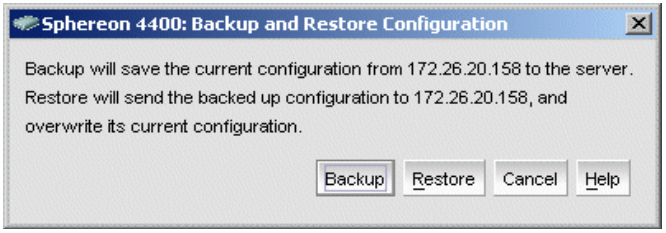

Sphereon 4400: Backup and Restore Configuration
Backup will save the current configuration from 172.26.20.158 to the server.
Restore will send the backed up configuration to 172.26.20.158, and
overwrite its current configuration.
Backup
Restore
Cancel
Help

Figure 4-19 Backup and Restore Configuration Dialog Box

2. Click *Backup*. An *Information* dialog box appears, indicating the backup was initiated.
3. Click *OK* to complete the backup and close the dialog box.

Restore Configuration

To restore the switch configuration file from the management server:

Inform the customer the switch is to be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.

1. Set the switch offline. For instructions, refer to *Setting Online State*.
2. Select *Backup & Restore Configuration* from the *Maintenance* menu(*Maintenance>Backup&Restore Configuration*). The *Backup and Restore Configuration* dialog box appears (Figure 4-19).
3. Click *Restore*. A *Warning* dialog box appears, indicating the existing configuration file is to be overwritten.
4. Click *Yes*. A *Restore* dialog box appears, indicating the restore is in progress.

   When the operation finishes, the *Restore* dialog box appears a **Restore complete** message.
5. Click *Close* to close the dialog box.

Reset Configuration Data

When configuration data is reset to factory default values, the switch defaults to the factory-set (Internet Protocol) IP address and all optional features are disabled. To reset configuration data to factory default settings:

Inform the customer the switch is to be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.

1. Set the switch offline. For instructions, refer to *Setting Online State*.
2. At the SAN management application's physical map, right-click the product icon representing the switch for which a configuration file is to be reset to factory default settings, then select *Element Manager* from the pop-up menu. The application opens.
3. Select *Reset Configuration* from the *Maintenance* menu (*Maintenance>Reset Configuration*). The *Reset Configuration* dialog box appears (Figure 4-20).

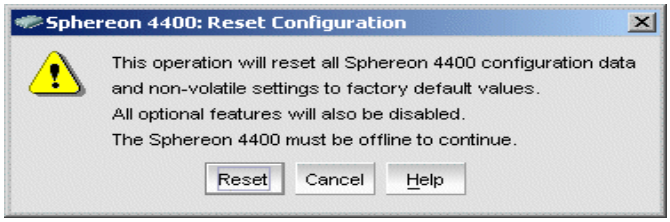

Sphereon 4400: Reset Configuration
This operation will reset all Sphereon 4400 configuration data
and non-volatile settings to factory default values.
All optional features will also be disabled.
The Sphereon 4400 must be offline to continue.
Reset
Cancel
Help

Figure 4-20 Reset Configuration Dialog Box

4. Click *Reset* to initiate the reset operation and close the dialog box.
5. The switch IP address resets to the default address of **10.1.1.10**.
   - — If the configured IP address (prior to reset) was the same as the default address, the switch-to-management server Ethernet link is not affected and the procedure is complete.
   - — If the configured IP address (prior to reset) was not the same as the default address, the switch-to-management server Ethernet link drops and server communication is lost. Continue to the next step.
6. To change the switch IP address and restart the management server session, go to step 7. To restart a management server session using the default IP address of **10.1.1.10**:
   a. Close the Element Manager application and return to the SAN management application.

   A grey square with a yellow exclamation mark appears adjacent to the icon representing the reset switch, indicating switch is not communicating with the management server.

   b. Select *Setup* from the *Discover* menu(*Discover>Setup*). The *Discover Setup* dialog box appears (Figure 4-21).

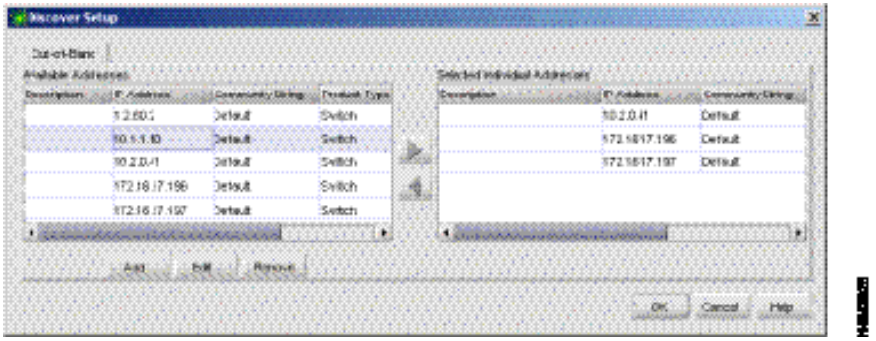


Figure 4-21 Discover Setup Dialog Box

c. Select (highlight) the entry representing the reset switch in the *Available Addresses* window and click *Edit*. The *Address Properties* dialog box appears (Figure 4-22).

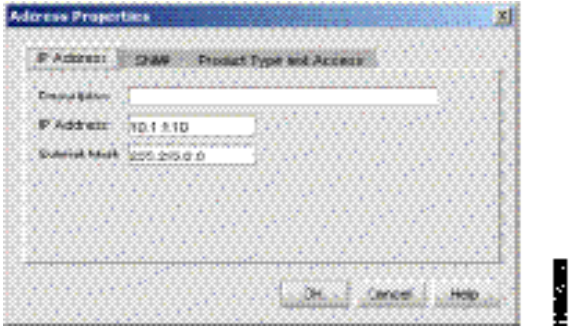


Figure 4-22 Address Properties Dialog Box

d. Type **10.1.1.10** in the *IP Address* field and click *OK*. Entries at the *Discover Setup* dialog box reflect the new IP address.

e. At the *Discover Setup* dialog box, click *OK*. Switch-to-management server communication is restored and the procedure is complete.

7. Change the switch IP address and restart the management server session as follows:

a. A grey square with a yellow exclamation mark appears adjacent to the icon representing the reset switch, indicating switch is not communicating with the management server.

b. Delete the icon representing the reset switch. At the SAN management application, select *Setup* from the *Discover* menu. The *Discover Setup* dialog box appears (Figure 4-21).

c. Select (highlight) the entry representing the reset switch in the *Available Addresses* window and click *Remove*.

d. click *OK* at the *Discover Setup* dialog box. The switch is no longer defined to the management server.

e. Change the switch IP address through the maintenance port. Refer to *Task 5: Configure Product Network Information (Optional)* for instructions.

f. Identify the switch to the SAN management application. Refer to *Task 13: Configure the Product to the Management Application* for instructions.

Installing or Upgrading Software

The delivered SAN management application is provided on the *EFC Management Applications* CD-ROM. Subsequent software versions for upgrade are provided to customers through the McDATA Filecenter.

NOTE: When upgrading software, follow all procedural information contained in release notes or EC instructions that accompany the version. Such information supplements information provided in this general procedure.

To install or upgrade the SAN management application:

1. Close and exit all applications, then perform one of the following:
   — Insert the *EFC Management Applications* CD-ROM into the CD-ROM drive of the server.
   — Ensure the desired software version is obtained from the Filecenter and resident on the server hard drive. Refer to *Download Firmware or Software from the Filecenter* for instructions.
2. At the server's Windows desktop, click *Start* at the left side of the task bar, then select the *Run* option. The *Run* dialog box appears.
3. In the *Open* field at the *Run* dialog box, type:

— **`C:\mcdataServerInstall.exe`** to install from the server hard drive.

— **`D:\mcdataServerInstall.exe`** to install from the *EFC Management Applications* CD-ROM.

4. Click *OK*. The *InstallShield* third-party application prepares to install the software version, and opens the *InstallShield Wizard* dialog box (Figure 4-23).

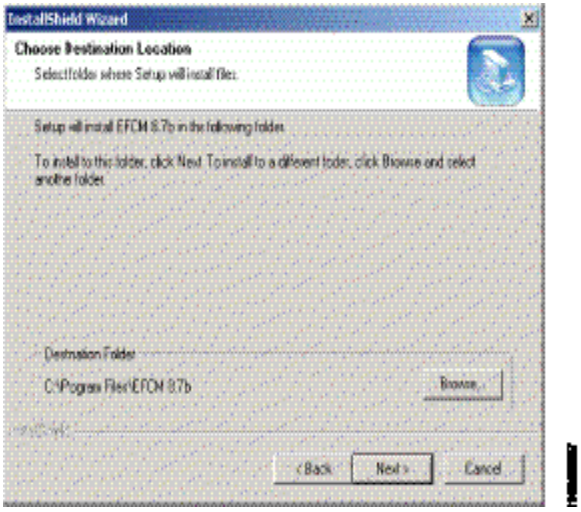

InstallShield Wizard
Choose Destination Location
Select folder where Setup will install files.
Setup will install EFCM 8.7b in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\EFCM 8.7b
Browse...
< Back
Next >
Cancel

Figure 4-23 InstallShield Wizard Dialog Box

5. Follow the online instructions for the *InstallShield Wizard*. Click *Next* and *Finish* as appropriate.
6. Power off and reboot the server.
   a. At the Windows desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box appears.
   b. Select the *Restart* option from the list box and click *OK*. The server powers down and restarts. During the reboot process the LAN connection between the server and browser-capable PC drops momentarily, and the TightVNC viewer appears a network error.

c. After the server reboots, click *Login again*. The *VNC Authentication* screen appears.

d. Type the default password and click *OK*. The *Welcome to Windows* dialog box appears.

NOTE: The default TightVNC viewer password is **password.**

e. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the server desktop. The *Log On to Windows* dialog box appears.

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the rack-mount management server.

f. Type the default Windows user name and password and click *OK*. The server's Windows desktop opens and the *EFCM Log In* dialog box appears.

NOTE: The default Windows user name is **Administrator** and the default password is **password**. Both are case-sensitive.

g. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default SAN management application user ID is **Administrator** and the default password is **password.** Both are case-sensitive.

h. Click *Login*. The application opens and the main window appears.

5

Removal and Replacement Procedures

This chapter describes field-replaceable unit (FRU) removal and replacement procedures (RRPs) for the Sphereon 4400 Fabric Switch. The chapter also provides procedural notes, electrostatic discharge (ESD) precautions, and list of FRUs.

Procedural Notes

Observe the following procedural notes:

1. Follow all ESD precautions and **DANGER**, **CAUTION**, and **ATTENTION** statements.
2. Do not perform an RRP unless a failure is isolated to a FRU. If fault isolation was not performed, refer to *MAP 0000: Start MAP*.
3. Before removing a FRU, read the associated RRP to familiarize yourself with the procedure.
4. After completing an RRP:
   - — Clear the event codes reporting the failure and recovery from the product *Event Log*.
   - — Extinguish the amber system error light-emitting diode (LED) at the product front panel.

ESD Procedures

Follow these ESD procedures:

- If the product is connected to facility power (grounded), wear an ESD wrist strap and grounding cable connected to the product chassis.
- If the product is not connected to facility power (not grounded), wear an ESD wrist strap and grounding cable connected to an approved bench grounding point.
- Touch the product chassis once before performing a procedure, and once each minute during the procedure.
- Store ESD-sensitive FRUs in antistatic packaging.

Field-Replaceable Units

Table 5-1 lists concurrent FRUs that are removed and replaced while the product is powered on and operational. The table also lists ESD precautions (yes or no) for each FRU, and references the RRP page number. Refer to Chapter 6, *Illustrated Parts Breakdown* for FRU locations and part numbers.

Table 5-1 Concurrent FRUs

Concurrent FRU	ESD Requirement	Page
Small form factor pluggable optical transceiver	Yes	5-3
Redundant power supply	No	5-7

RRP 1: SFP Optical Transceiver

Use the following procedures to remove or replace a small form factor pluggable (SFP) optical transceiver. A list of required tools is provided.

Tools Required

The following tools are required:

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- Protective cap (provided with the fiber-optic jumper cable).
- Loopback plug (provided with the product).
- Fiber-optic cleaning kit.
- ESD grounding cable and wrist strap.

Removal

To remove an SFP optical transceiver:

1. Inform the customer the port with the defective transceiver will be blocked. Ensure the system administrator sets any attached device offline.
2. If the product is not rack-mounted, go to step 3. If the product is rack-mounted, perform one of the following:
   - — If the product is installed in an FC-512 Fabricenter equipment cabinet, insert the 5/16-inch door tool into the socket hole at the right top of the door (front or rear). Turn the tool counter-clockwise to unlock and open the door.
   - — If the product is installed in a customer-supplied equipment cabinet, unlock and open the cabinet door (front or rear) as directed by the customer representative.
3. Identify the defective port transceiver from:
   - — An illuminated amber LED adjacent to the port.
   - — At a web browser communicating with the EFCM Basic Edition interface, port failure information displayed at the *Hardware View*, *Port List View*, or *Event Log*.
   - — At the management server (Element Manager application), port failure information displayed at the *Hardware View*, *Port List View*, *Port Properties* dialog box, or *Event Log*.

4. Block communication to the port. Refer to *Blocking or Unblocking a Port* (EFCM Basic Edition) or *Blocking or Unblocking a Port* (SAN management application) for instructions.
5. Ensure an ESD grounding cable is connected to the product chassis (or approved bench ground) and your wrist.
6. Disconnect the fiber-optic jumper cable from the port:
   a. Pull the keyed LC connector free from the port's optical transceiver.
   b. Place a protective cap over the jumper cable connector.
7. The optical transceiver has a wire locking bale to secure the transceiver in the port receptacle and to assist in removal. The bale rotates up or down, depending on transceiver manufacturer and port location (top or bottom row).
   a. Disengage the locking mechanism by rotating the wire bale up or down 90 degrees as shown in part (1) of Figure 5-1.
   b. Grasp the wire bale and pull the transceiver from the port receptacle as shown in part (2) of Figure 5-1.

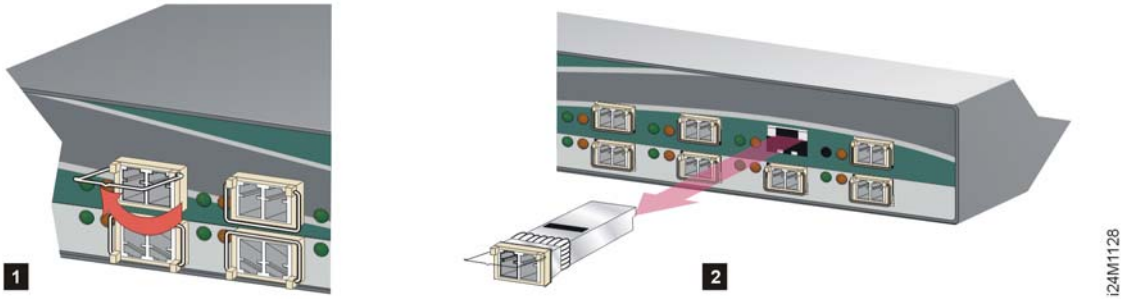


Figure 5-1 SFP Optical Transceiver Removal and Replacement

8. Inspect the *Event Log*:
   — At a web browser communicating with the EFCM Basic Edition interface, select *Event* from the *Logs* menu.
   — At the management server (Element Manager application), select *Event Log* from the *Logs* menu.

   An event code **513** (SFP optics hot-removal completed) appears in the *Event Log*.

Replacement

To replace an SFP optical transceiver:

1. Ensure an ESD grounding cable is connected to the product chassis (or approved bench ground) and your wrist.
2. Remove the replacement transceiver from its packaging.
3. Insert the transceiver into the port receptacle, then engage the locking mechanism by rotating the wire bale up or down 90 degrees as shown in Figure 5-1.
4. Perform an external loopback test. Refer to *External Loopback Test* (EFCM Basic Edition) or *External Loopback Test* (SAN management application) for instructions. If the test fails, go to *MAP 0000: Start MAP* to isolate the problem.
5. Reconnect the fiber-optic jumper cable:
   a. Remove the protective cap from the cable connector and the protective plug from the port optical transceiver. Store the cap and plug in a suitable location for safekeeping.
   b. Clean the jumper cable and transceiver connectors. Refer to *Clean Fiber-Optic Components* for instructions.
   c. Insert the keyed LC cable connector into the port's optical transceiver.
6. Ensure the amber port LED extinguishes. If the LED illuminates, go to *MAP 0000: Start MAP* to isolate the problem.
7. Inspect the *Event Log*:
   — At a web browser communicating with the EFCM Basic Edition interface, select *Event* from the *Logs* menu.
   — At the management server (Element Manager application), select *Event Log* from the *Logs* menu.

   Ensure an event code **510** (SFP optics hot-insertion initiated) appears. If the event code does not appear, go to *MAP 0000: Start MAP* to isolate the problem.
8. Verify port operation:
   — At a web browser communicating with the EFCM Basic Edition interface, open the *Hardware View*:
      a. Ensure alert symbols do not appear (yellow triangle or red diamond).

b. Open the *Port List View*. Verify that port *Operational State*, *Type*, *Health Status*, and *Transceiver* are correct.

— At the management server (Element Manager application), open the *Hardware View*:

a. Ensure alert symbols do not appear (yellow triangle or red diamond).

b. Double-click the port graphic to open the *Port Properties* dialog box. Verify port information is correct.

c. Right-click the port graphic and select *Port Technology* from the menu. The *Port Technology* dialog box displays. Verify the port technology is correct.

If a problem is indicated, go to *MAP 0000: Start MAP* to isolate the problem.

9. Restore communication to the port as directed by the customer. Refer to *Blocking or Unblocking a Port* (EFCM Basic Edition) or *Blocking or Unblocking a Port* (SAN management application) for instructions. Inform the customer the port is available.

10. Clear the system error LED on the product front bezel:

— At a web browser communicating with the EFCM Basic Edition interface, select *Clear System Error Light* from the *Maintenance* menu.

— At the management server (Element Manager application), open the *Hardware View*. Right-click the front panel bezel graphic (away from a FRU), then click the *Clear System Error Light* menu selection.

11. If necessary, close and lock the equipment cabinet door.

RRP 2: Redundant Power Supply

Use the following procedures to remove or replace a redundant external power supply. A list of required tools is provided.

Tools Required

A door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet) is required.

Removal

To remove a redundant external power supply:

1. If the product is not rack-mounted, go to step 2. If the product is rack-mounted, perform one of the following:
   - — If the product is installed in an FC-512 Fabricenter equipment cabinet, insert the 5/16-inch door tool into the socket hole at the right top of the door (front or rear). Turn the tool counter-clockwise to unlock and open the door.
   - — If the product is installed in a customer-supplied equipment cabinet, unlock and open the cabinet door (front or rear) as directed by the customer representative.
2. Identify the defective power supply from:
   - — The extinguished green LED on the FRU.
   - — At a web browser communicating with the EFCM Basic Edition interface or at the management server (Element Manager application), FRU failure information displayed at the *Hardware View*, *FRU List View*, or *Event Log*.
3. Disconnect the AC power cord from facility power.

DANGER

Disconnect the power cords. (D005)

4. Twist the external power supply adapter cord counterclockwise to unlock the connection, then disconnect the cord from the threaded output jack at the rear of the switch chassis as shown in Figure 5-2. Remove the power supply.

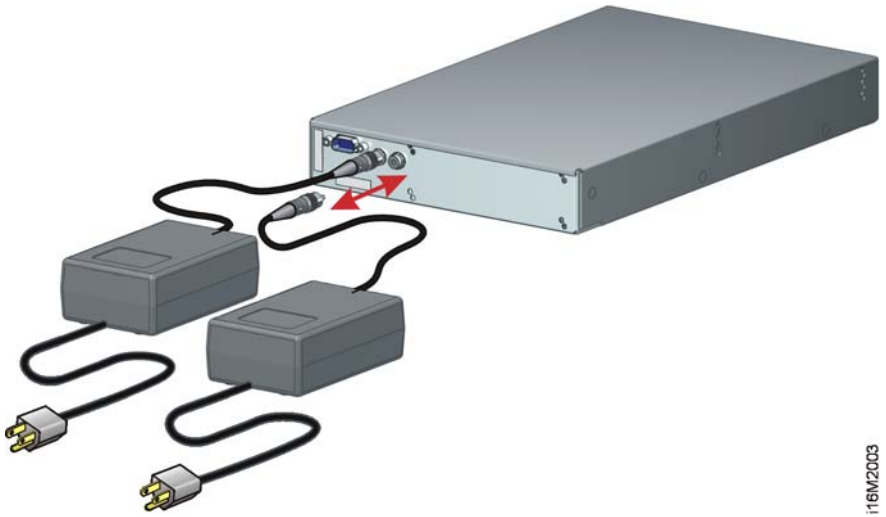


Figure 5-2 Redundant Power Supply Removal and Replacement

5. Inspect the *Event Log*:
   - — At a web browser communicating with the EFCM Basic Edition interface, select *Event* from the *Logs* menu.
   - — At the management server (Element Manager application), select *Event Log* from the *Logs* menu.

   The following event codes appear:
   - **200 -** Power supply AC voltage failure (recorded when power is disconnected).
   - **206 -** Power supply removed.

Replacement

To replace a redundant power supply:

1. Remove the replacement power supply from its packaging.
2. Connect the power supply adapter cord to the threaded output jack at the rear of the switch chassis as shown in Figure 5-2. Twist the cord clockwise to lock and secure the connection.
3. Connect the AC power cord to a facility power source.
4. Wait several seconds, then inspect the power supply to ensure the amber LED extinguishes. If the LED illuminates, go to *MAP 0000: Start MAP* to isolate the problem.

5. Inspect the *Event Log*:

   — At a web browser communicating with the EFCM Basic Edition interface, select *Event* from the *Logs* menu.

   — At the management server (Element Manager application), select *Event Log* from the *Logs* menu.

   Ensure the following event codes appear:

   - **203 -** Power supply AC voltage recovery.
   - **207 -** Power supply installed.

   If the event codes do not appear, go to *MAP 0000: Start MAP* to isolate the problem.

6. Verify power supply operation. At a web browser communicating with the EFCM Basic Edition interface or at the management server (Element Manager application), open the *Hardware View* and observe the FRU graphic to ensure alert symbols do not appear (yellow triangle or red diamond).

   If a problem is indicated, go to *MAP 0000: Start MAP* to isolate the problem.

7. Perform a data collection procedure. Refer to *Collecting Maintenance Data* (EFCM Basic Edition) or *Collecting Maintenance Data* (SAN management application) for instructions.

8. Clear the system error LED on the product front bezel:

   — At a web browser communicating with the EFCM Basic Edition interface, select *Clear System Error Light* from the *Maintenance* menu.

   — At the management server (Element Manager application), open the *Hardware View*. Right-click the front panel bezel graphic (away from a FRU), then click the *Clear System Error Light* menu selection.

9. If necessary, close and lock the equipment cabinet door.

6

Illustrated Parts Breakdown

This chapter provides an illustrated parts breakdown for Sphereon 4400 Fabric Switch field-replaceable units (FRUs). Exploded-view assembly drawings are provided for:

- Front-accessible FRUs.
- Rear-accessible FRUs.
- Miscellaneous parts.
- Power cords and receptacles.

Exploded-view illustrations portray the switch disassembly sequence for clarity. Illustrated FRUs are numerically keyed to associated tabular part lists. The lists also include part numbers, descriptions, and quantities.

RoHS Information

European Parliament Directive 2002/95/EC takes effect July 1, 2006 restricting the use of certain hazardous substances in electrical and electronic equipment (RoHS). Equipment placed on the market before that date is exempt from RoHS regulations. The use of non-RoHS parts for repair and replacement is permitted for non-RoHS equipment. Equipment placed on the market after that date must comply with RoHS regulations, including the requirement that all repairs and replacements must use parts that are RoHS compliant

Front-Accessible FRUs

Figure 6-1 illustrates front-accessible FRUs. Table 6-1 is the associated FRU parts list. The table includes reference numbers to Figure 6-1, FRU part numbers, descriptions, and quantities.

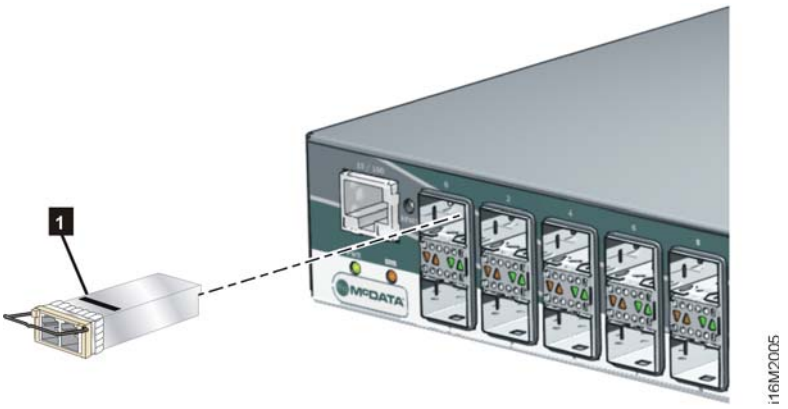


Figure 6-1 Front-Accessible FRUs

Table 6-1 Front-Accessible FRU Parts List

Ref.	ROHs Part Number	Non-ROHs Part Number	Description	Qty.
6 - 1	002-E02774	002-002774-000	Switch, Sphereon 4400, base assembly	Reference
-1	803-E00084	803-000084-386	Transceiver, optical, SFP, 850 nm, 3.3 volt, LC connector, tri-rate (1.0625/2.1250/4.2500 Gbps), digital diagnostic	0 to 16
-1	803-E00085	N/A	Transceiver, optical,LW 4 Gpbps 4km SPFP	0 to 16
-1	803-E00086	N/A	Transceiver, optical,LW 4 Gpbps 10km SPFP	0 to 16

Rear-Accessible FRUs

Figure 6-2 illustrates rear-accessible FRUs. Table 6-2 is the associated FRU parts list. The table includes reference numbers to Figure 6-2, FRU part numbers, descriptions, and quantities.

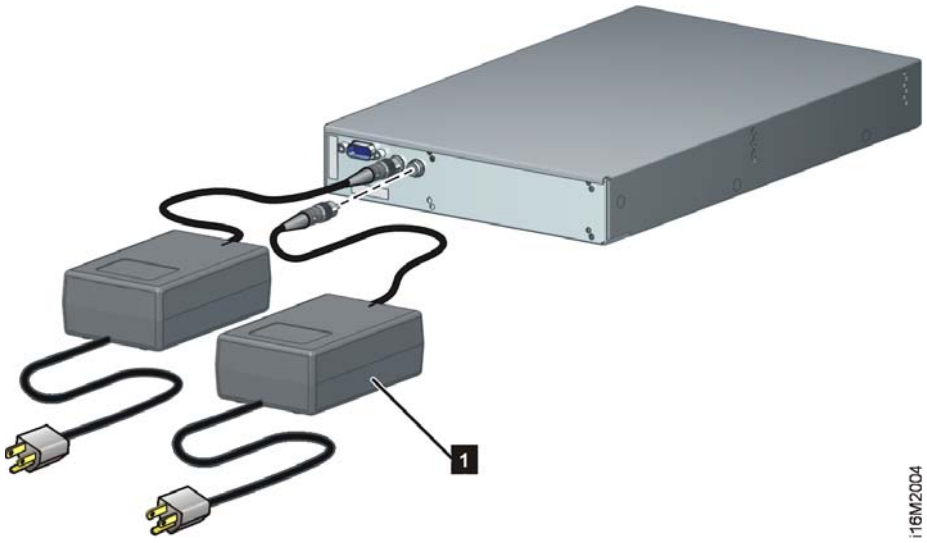


Figure 6-2 Rear-Accessible FRUs

Table 6-2 Rear-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
6 - 2	002-002774-000	Switch, Sphereon 4400, base assembly	Reference
-1	721-000105-000	Power supply assembly, external, 60-watt rated, 12 VDC output	2

Miscellaneous Parts

Figure 6-3 illustrates miscellaneous parts. Table 6-3 is the associated parts list. The table includes reference numbers to Figure 6-3, part numbers, descriptions, and quantities.

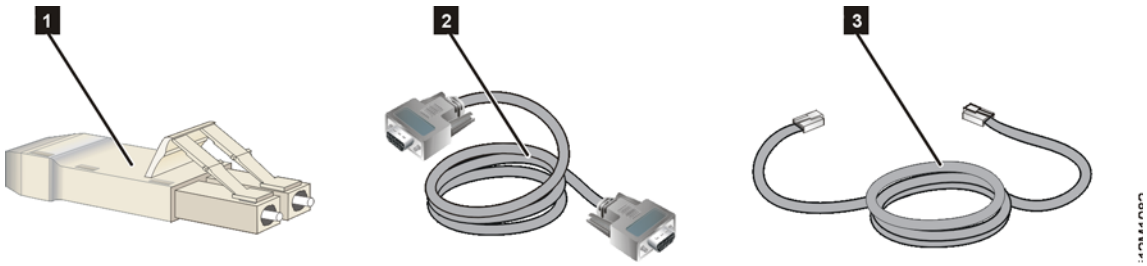


Figure 6-3 Miscellaneous Parts

Table 6-3 Miscellaneous Parts List

Ref.	Part Number	Description	Qty.
-1	803-000057-000	Plug, loopback, LC connector, multimode, 50/125 micron (#1148)	1
-2	801-000039-000	Cable, communication, null modem, DB9F-DB9F connectors, 10-foot	1
-3	801-000035-010	Cable, Ethernet, RJ-45 connectors, Category 5E, 10-foot	1

Power Cords and Receptacles

Figure 6-4 illustrates optional power cords and receptacles. Table 6-4 is the associated parts list. The table includes reference numbers to Figure 6-4, feature numbers, and descriptions.

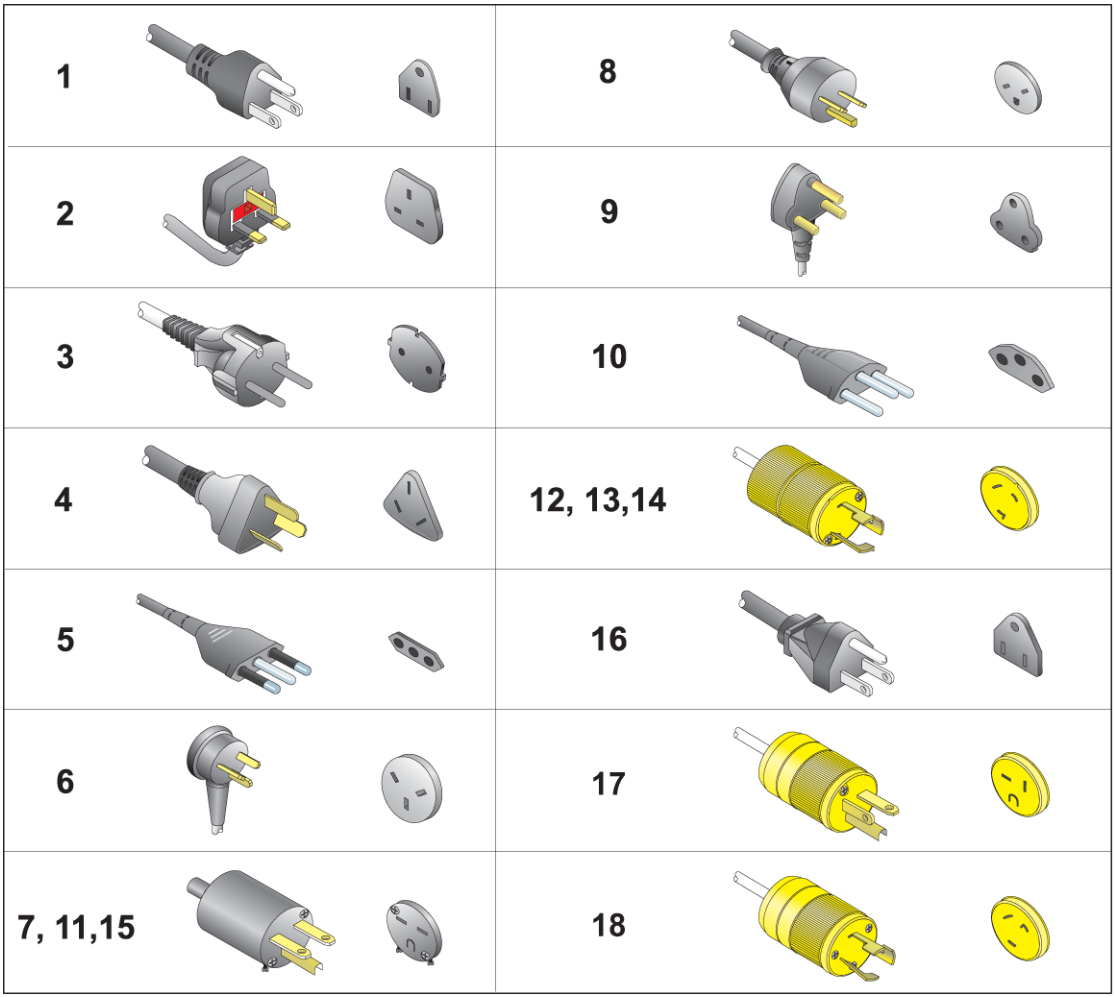


Figure 6-4 Power Cords and Receptacles

Table 6-4 Power Cord and Receptacle List

Ref.	Part Number	Description	Feature
-1	806-000001-000	Power cord, AC, North America NEMA 5-15P straight, 125 volts, 10 amps, 3.0 meters Receptacle: NEMA 5-15R	1010
-2	806-000004-001	Power cord, AC, United Kingdom BS 1363 right angle, 250 volts, 10 amps, 2.8 meters Receptacle: BS 1363	1012
-3	806-000005-001	Power cord, AC, European Union CEE 7/7 straight, 250 volts, 10 amps, 2.8 meters Receptacle: CEE 7	1013
-4	806-000006-001	Power cord, AC, Australia AS 3112 straight, 250 volts, 10 amps, 2.8 meters Receptacle: AS 3112	1014
-5	806-000027-000	Power cord, AC, Italy, Chile, Libya, and Ethiopia CEI 23-16/VII straight, 250 volts, 10 amps, 2.8 meters Receptacle: CEI 23-16/VII	1021
-6	806-000029-000	Power cord, AC, Israel SI-32 right angle, 250 volts, 15 amps, 2.8 meters Receptacle: SI-32	1022
-7	806-000030-000	Power cord, AC, Thailand, Philippines, Taiwan, Bolivia, and Peru NEMA 6-15P straight, 250 volts, 15 amps, 2.8 meters Receptacle: NEMA 6-15R	1023
-8	806-000033-000	Power cord, AC, Denmark Afsnit 107-2-D1 straight, 250 volts, 10 amps, 2.8 meters Receptacle: Afsnit 107-2-D1	1024
-9	806-000034-000	Power cord, AC, South Africa, Burma, Pakistan, India, and Bangladesh BS 546 Type, right angle, 250 volts, 15 amps, 2.8 meters Receptacle: BS 546	1025
-10	806-000037-000	Power cord, AC, Switzerland and Liechtenstein SEV 1011 straight, 250 volts, 10 amps, 2.8 meters Receptacle: SEV 1011	1026
-11	806-000038-000	Power cord, AC, United States (Chicago) NEMA 6-15P straight, non-locking, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA 6-15R	1027

Table 6-4 Power Cord and Receptacle List (Continued)

Ref.	Part Number	Description	Feature
-12	806-000040-000	Power cord, AC, United States (Chicago) NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA L6-15R	1028
-13	806-000042-000	Power cord, AC, North America NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA L6-15R	1016 and 1029
-14	806-000043-000	Power cord, AC, Japan NEMA 6-15P straight, 240 volts, 6 amps, 2.8 meters Receptacle: NEMA 6-15R **Note:** The power cord shipped is specifically intended for use with the associated product and cannot be used with any other electrical products.	1030
-15	806-000058-000	Power cord, AC, Japan JIS 8303 straight, 125 volts, 12 amps, 2.5 meters Receptacle: NEMA 5-15R **Note:** The power cord shipped is specifically intended for use with the associated product and cannot be used with any other electrical products.	None
-17	806-E00080-004	Power cord, North America NEMA 6-20P, right angle, non-locking, 250 volts, 20 amps, 4.3 meters Receptacle: NEMA 6-20R	1078
-18	806-E00081-004	Power cord. North America NEMA L6-20P, right angle, twist-lock, 250 volts, 16 amps, 4.3 meters Receptacle: NEMA L6-20R	1078

Power Cords (Japan, Denan)

注意 – 添付の電源コードを他の装置や用途に使用しない
添付の電源コードは本装置に接続し、使用することを目的として設計され、その安全性が確認されているものです。決して他の装置や用途に使用しないでください。火災や感電の原因となる恐れがあります。

CAUTION

Never use the power cord packed with your equipment for other products.

A

Event Code Tables

An event is a state change, problem detection, or problem correction that requires attention or should be reported to service personnel. An event usually indicates an operational state transition, but may also indicate an impending state change (threshold violation) or provide information only. Events are reported as event codes. This appendix lists three-digit event codes. The codes are listed in numerical order and tabular format as follows:

- **000** through **199** - system events.
- **200** through **299** - power supply events.
- **300** through **399** - fan events.
- **400** through **499** - control processor (CTP) card events.
- **500** through **599** - port events.
- **800** through **899** - thermal sensor events.

Events are recorded in the *Event Log* at the Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface or rack-mount management server (Element Manager application). An event illuminates the system error light-emitting diode (LED) at the product front panel.

Tables in this appendix also provide a:

- **Message -** a text string that describes the event.
- **Severity -** a severity level that indicates event criticality as follows:

— **0 -** informational.

— **2 -** minor.

— **3 -** major.

— **4 -** severe (not operational).

- **Explanation -** an explanation of what caused the event.
- **Action -** the recommended course of action (if any) to resolve the problem.
- **Event data -** supplementary event data (if any) that appears in the event log in hexadecimal format.
- **Distribution -** checks in associated fields indicate where the event code is reported (product, management server, or attached host).

System Events (000 through 199)

Event Code: 011							
Message:	Login Server database invalid.						
Severity:	Minor.						
Explanation:	Following an initial machine load (IML) or firmware download, the Login Server database failed cyclic redundancy check (CRC) validation. All fabric service databases initialize to an empty state, resulting in implicit fabric logout of all attached devices.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔		

Event Code: 021							
Message:	Name Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Name Server database failed CRC validation. All fabric service databases initialize to an empty state, resulting in implicit fabric logout of all attached devices.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔		

Event Code: 031							
Message:	SNMP request received from unauthorized community.						
Severity:	Informational.						
Explanation:	An SNMP request containing an unauthorized community name was rejected with an error. Only requests containing authorized SNMP community names configured through the Element Manager application are allowed.						
Action:	Add the community name to the SNMP configuration using the Element Manager application.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 051							
Message:	Management Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Management Server database failed CRC validation. All management service databases initialize to an empty state, resulting in implicit logout of all logged-in devices.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔		

Event Code: 061							
Message:	Fabric Controller database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the fabric controller database failed CRC validation. All fabric controller databases initialize to an empty state, resulting in momentary loss of interswitch communication.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔		

Event Code: 062							
Message:	Maximum interswitch hop count exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller software detected a path to a director or switch that traverses more than seven interswitch links (hops). This may result in Fibre Channel frames persisting in the fabric longer than timeout values allow.						
Action:	Reconfigure the fabric so the path between any two switches traverses seven or less ISLs.						
Event Data:	Byte **0** = domain ID of the director or switch more than seven hops away.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 063							
Message:	Remote switch has too many ISLs.						
Severity:	Major.						
Explanation:	The director or switch with domain ID indicated in the event data has too many ISLs attached and is unreachable from this switch. SAN management application Version 3.2 and earlier supports up to 32 ISLs. SAN management application Version 3.3 and later supports up to 128 ISLs.						
Action:	Reduce the ISLs on the indicated director or switch to a number within limits specified.						
Event Data:	Byte **0** = domain ID of the director or switch with too many ISLs.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔			

Event Code: 064							
Message:	ESS response from indicated domain ID not received after maximum tries.						
Severity:	Informational.						
Explanation:	Fabric controller software detected an exchange switch support (ESS) response from the indicated domain ID was not received after the maximum attempts. The event is reported only in McDATA interop mode.						
Action:	No action required.						
Event Data:	Byte **0** = domain ID of the director or switch not receiving an ESS response. Byte **1** = domain ID of the director or switch not responding.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 070							
Message:	E_Port is segmented.						
Severity:	Informational.						
Explanation:	An E_Port recognized an incompatibility with the attached director or switch, preventing fabric participation. A segmented port does not transmit Class 2 or Class 3 traffic, but transmits Class F traffic. Refer to event data for segmentation reason.						
Action:	Action depends on segmentation reason specified.						
Event Data:	The first byte of event data (byte **0**) specifies the E_Port number. The fifth byte (byte **4**) specifies the segmentation reason as follows: **1 = Incompatible operating parameters -** Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another director or switch. Modify the R_A_TOV and E_D_TOV to make the values consistent. **2 = Duplicate domain ID -** The switch has the same preferred domain ID as another director or switch) Modify the Domain ID to make it unique. **3 = Incompatible zoning configurations -** The same name is applied to a zone for the switch and another director or switch, but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members. **4 = Build fabric protocol error -** A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform a data collection and return the CD to support personnel. **5 = No principal switch -** No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255. **6 = No response from attached switch (hello timeout) -** The switch periodically verifies operation of attached directors or switches. The E_Port at the operational switch times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform a data collection and return the CD to support personnel.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔	✔			

Event Code: 071							
Message:	Switch is isolated.						
Severity:	Informational.						
Explanation:	The switch is isolated from other directors or switches. This event code is accompanied by one or more **070** event codes. Refer to event data for segmentation reason.						
Action:	Action depends on segmentation reason specified.						
Event Data:	The first byte of event data (byte **0**) specifies the E_Port number. The fifth byte (byte **4**) specifies the segmentation reason as follows: **1 = Incompatible operating parameters -** Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another director or switch. Modify the R_A_TOV and E_D_TOV to make the values consistent. **2 = Duplicate domain ID -** The switch has the same preferred domain ID as another director or switch) Modify the Domain ID to make it unique. **3 = Incompatible zoning configurations -** The same name is applied to a zone for the switch and another director or switch, but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members. **4 = Build fabric protocol error -** A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform a data collection and return the CD to support personnel. **5 = No principal switch -** No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255. **6 = No response from attached switch (hello timeout) -** The switch periodically verifies operation of attached directors or switches. The E_Port at the operational switch times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform a data collection and return the CD to support personnel.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 072							
Message:	E_Port connected to unsupported switch.						
Severity:	Informational.						
Explanation:	The switch is attached (through an ISL) to an incompatible director or switch.						
Action:	Disconnect the ISL.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 073							
Message:	Fabric initialization error.						
Severity:	Informational.						
Explanation:	An error was detected during the fabric initialization sequence, probably caused by frame delivery errors. Event data is intended for engineering evaluation.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	Byte **0** = error reason code for engineering evaluation. Bytes **4** - **9** = port numbers where problems were detected.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 074							
Message:	ILS frame delivery error threshold exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller frame delivery errors exceeded an E_Port threshold and caused fabric initialization problems (**073** event code). Most problems are caused by control frame delivery errors, as indicated by this code. Event data is intended for engineering evaluation.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	Byte **0** = E_Port number reporting the problem. Bytes **4** - **8** = Count of frame delivery timeouts. Bytes **9** - **11** = Count of frame delivery aborts.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 075							
Message:	E_Port segmentation recovery.						
Severity:	Informational.						
Explanation:	A segmented E_Port (event code **070**) recovered. This event is not generated if the port is manually recovered by blocking and unblocking, setting offline and online, or disconnecting the fiber-optic cable.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the E_Port number. The fifth byte (byte **4**) specifies the original segmentation reason as described in event code **070**.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔	✔			

Event Code: 076							
Message:	Out of Range Domain ID detected.						
Severity:	Informational.						
Explanation:	Switch has detected a domain ID that is out of the supported range behind the attached ISL. This event may be followed by a segmentation event 070.						
Action:	Check that all McDATA switches in the fabric are configured with the same domain id offset. Check that all non-McDATA switches are configured with a domain id that is within the range of this switch (offset + 1 ' offset + 31).						
Event Data:	Byte **0** = E Port number. Byte **1** = Out of Range Domain ID Bytes **8** - **15** = WWNN of Switch with Out of Range Domain ID.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔	✔			

Event Code: 080							
Message:	Unauthorized worldwide name.						
Severity:	Informational.						
Explanation:	The WWN of the connected device or fabric element is not authorized for the port number.						
Action:	Change the port binding definition or connect the proper device or fabric element to the indicated port.						
Event Data:	Byte **0** = Port number reporting the unauthorized connection. Bytes **4** - **11** = WWN of the unauthorized device or fabric element.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔	✔			

Event Code: 081	
Message:	Invalid attachment.
Severity:	Informational.
Explanation:	A switch port recognized an incompatibility with the attached fabric element or device and isolated the port. An isolated port does not transmit Class 2, Class 3, or Class F traffic. Refer to event data for the reason.
Action:	Action depends on reason specified.
Event Data:	The first byte of event data (byte **0**) specifies the port number. The fifth byte (byte **4**) specifies the isolation reason as follows: **1 = Unknown -** Reason is unknown, but probably caused by failure of an E_Port connected device. Fault isolate the failed device or contact support personnel to report the problem. **2 = ISL connection not allowed -** The port connection conflicts with the configured port type. Change the port type to **F_Port** if the port is cabled to a device, or **E_Port** if the port is cabled to a fabric element to form an ISL. **3 = Incompatible switch -** The switch returned a *Process ELP Reject - Unable to Process* reason code because the attached fabric element is not compatible. Set the switch operating mode to **McDATA Fabric 1.0** if connected to a McDATA product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor. **4 = Incompatible switch -** The switch returned a *Process ELP Reject - Invalid Revision Level* reason code because the attached fabric element is not compatible. Set the switch operating mode to **McDATA Fabric 1.0** if connected to a McDATA product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor. **5 = Loopback plug connected -** A loopback plug is connected to the port with no diagnostic test running. Remove the loopback plug. **6 = N_Port connection not allowed -** The switch is connected to a fabric element through a misconfigured port. Change the port type to **E_Port**. **7 = Non-McDATA switch at other end -** The attached fabric element is not a McDATA product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor. **8 = E_Port capability disabled -** The product does not have E_Port capability. Enable this functionality through the appropriate product feature enablement (PFE) key.

Event Code: 081 (continued)	
Event Data (continued):	**A = Unauthorized port binding WWN -** The device WWN or nickname used to configure port binding for this port is not valid. At the *Configure Ports* dialog box, reconfigure the port with the WWN or nickname authorized for the attached device, or disable the port binding feature. **B = Unresponsive node -** The attached node did not respond, resulting in a G_Port ELP timeout. Check the status of the attached device and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem. **C = ESA security mismatch -** Processing of the Exchange Security Attribute (ESA) frame detected a security feature mismatch. The switch binding parameters for this switch and the attached fabric element must agree. At the *Switch Binding - State Change* dialog boxes, ensure the parameters for both fabric elements are compatible, or disable the fabric and switch binding features. **D = Fabric binding mismatch -** Fabric binding is enabled and an attached fabric element has an incompatible fabric membership list. At the *Fabric Binding* dialog box, update the fabric membership list for both fabric elements to ensure compatibility, or disable the fabric binding feature. **E = Authorization failure reject -** The fabric element connected to the switch through an ISL detected a security violation. As a result, the switch received a generic reason code and set the port to an invalid attachment state. Check the port status of the attached fabric element and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem. **F = Unauthorized switch binding WWN -** Switch binding is enabled and an attached device or fabric element has an incompatible switch membership list. At the *Switch Binding - Membership List* dialog box, update the switch membership list for the switch and the attached device or fabric element to ensure compatibility, or disable the switch binding feature. **10 = Authentication failure -** An ISL challenge handshake authentication protocol (CHAP) check failed. Update the authentication list or disable the authentication feature. **11 = Fabric mode mismatch -** Based on the ELP revision level, a connection was not allowed because a McDATA switch in legacy mode is attached to a McDATA switch in Open Fabric mode, or a McDATA switch in Open Fabric mode is attached to an OEM switch at an incorrect ELP revision level. Update the fabric mode for one switch using the *Interop Mode* drop-down list at the *Configure Fabric Parameters* dialog box.

Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔			✔	

<table>
<tr><th colspan="8">Event Code: 082</th></tr>
<tr><td>Message:</td><td colspan="7">Port fenced.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">The port was blocked after exceeding threshold criteria defined by the port fencing policy. A hardware malfunction is indicated or the port fencing policy is too restrictive. The fence type is indicated in the event data.</td></tr>
<tr><td>Action:</td><td colspan="7">Identify and correct the hardware malfunction (port transceiver, fiber-optic cable, or attached fabric element), or change the port fencing threshold settings to more lenient values. After problem correction, unblock the port.</td></tr>
<tr><td>Event Data:</td><td colspan="7">The first byte of event data (byte 0) specifies the port number. The fifth byte (byte 4) specifies the fence type code as follows:

1 = Protocol error - Failure is associated with persistent incomplete operations or application-layer protocol errors (including port logins, fabric rebuilds, and management protocol errors).

2 = Link level hot I/O - Failure is hardware related and associated with an unstable link-state machine.

3 = Security violation - Failure is associated with persistent firmware-related security feature violations (port binding violations or authentication failures).

The ninth byte (byte 8) specifies the disabled reason code as follows:

1 = Unknown - The failure reason is unknown.

9 = ISL fencing - The E_Port (ISL) was fenced after the port exceeded a threshold value.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Product</td><td colspan="3">Management Server</td><td colspan="2">Host</td></tr>
<tr><td>EFCM Basic Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident Log</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td>✔</td><td></td></tr>
</table>

<table>
<tr><th colspan="8">Event Code: 083</th></tr>
<tr><td>Message:</td><td colspan="7">Port set to inactive state.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">A hardware or software problem prevented the port from coming online and set the port to an inactive state. Refer to event data for the inactive reason</td></tr>
<tr><td>Action:</td><td colspan="7">Action depends on inactive reason specified.</td></tr>
<tr><td>Event Data:</td><td colspan="7">The first byte of event data (byte 0) specifies the port number. The second byte (byte 1) specifies the inactive reason code as follows:

2 = Feature key not enabled - The optional flexport PFE key is not enabled.

3 = Switch speed conflict - The port cannot operated at the configured product (backplane or CTP Card) speed.

4 = Optics speed conflict - The port transceiver does not support the configured port speed.

5 = No SBAR - A serial crossbar (SBAR) is not installed. Not applicable to 4000-series fabric switches.

6 = Port swap conflict - The port swap configuration is invalid.

7=Sustained Mode User Configuration - The user has configured a neighboring port into sustained mode, thus preventing the use of this port

8=Virtualization engine initialization in progress-The virtualization engine is undergoing/awaiting initialization processing to conclude. Internal ports associated with the virtualization engine are inactive until initialization completes.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Product</td><td colspan="3">Management Server</td><td colspan="2">Host</td></tr>
<tr><td>EFCM Basic Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident Log</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td>✔</td><td></td></tr>
</table>

Event Code: 084							
Message:	Continuous Incident Detection and Reporting - threshold was exceeded for the port						
Severity:	Informational.						
Explanation:	CIDR threshold value exceeded for one of the following incidents • Unroutable Frames Incident - Port has received unroutable frames • Routable Good Frames Incident - Port has received frames with embedded port as destination • Invalid Transmission words Incident - Port has received invalid transmission words The CIDR reason code is indicated in the event data.						
Action:	Helps in identifying the misbehaving device, so that it could be corrected/fixed						
Event Data:	The first byte of event data (byte **0**) specifies the port number. The second byte (byte **1**) specifies the inactive reason code as follows: **1 = Unroutable Frames Incident -** The port has received unroutable frames. **2 = Good Frames Incident -** The port has received frames with embedded port as destination. **3 = Invalid Transmission Words Incident -** The port has received invalid transmission words.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

<table>
<tr><th colspan="8">Event Code: 085</th></tr>
<tr><td>Message:</td><td colspan="7">Continuous Incident Detection and Reporting with E-Mail - CIDR threshold was exceeded for the port and this event will trigger an E-Mail.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">CIDR threshold value exceeded for one of the following incidents
• Unroutable Frames Incident - Port has received unroutable frames
• Routable Good Frames Incident - Port has received frames with embedded port as destination
• Invalid Transmission words Incident - Port has received invalid transmission words

The CIDR reason code is indicated in the event data.</td></tr>
<tr><td>Action:</td><td colspan="7">Identify the responsible device and fix</td></tr>
<tr><td>Event Data:</td><td colspan="7">The first byte of event data (byte 0) specifies the port number. The second byte (byte 1) specifies the inactive reason code as follows:

1 = Unroutable Frames Incident - The port has received unroutable frames.

2 = Good Frames Incident - The port has received frames with embedded port as destination.

3 = Invalid Transmission Words Incident - The port has received invalid transmission words.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Product</td><td colspan="3">Management Server</td><td colspan="2">Host</td></tr>
<tr><td>EFCM Basic Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident Log</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td>✔</td><td></td><td></td><td></td></tr>
</table>

Event Code: 086							
Message:	Continuous Incident Detection and Reporting with Call Home - CIDR threshold was exceeded for the port and this event will trigger E-Mail as well as Call Home						
Severity:	Informational.						
Explanation:	CIDR threshold value exceeded for one of the following incidents • Unroutable Frames Incident - Port has received unroutable frames • Routable Good Frames Incident - Port has received frames with embedded port as destination • Invalid Transmission words Incident - Port has received invalid transmission words The CIDR reason code is indicated in the event data.						
Action:	Identify the responsible device and fix.						
Event Data:	The first byte of event data (byte **0**) specifies the port number. The second byte (byte **1**) specifies the inactive reason code as follows: **1 = Unroutable Frames Incident -** The port has received unroutable frames. **2 = Good Frames Incident -** The port has received frames with embedded port as destination. **3 = Invalid Transmission Words Incident -** The port has received invalid transmission words.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔	✔	✔		

Event Code: 120							
Message:	Error detected while processing system management command.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a management command that violates specified boundary conditions, typically as a result of a network error. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.						
Action:	No action is required for an isolated event. If this event persists, perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 121							
Message:	Zone set activation failed - zone set too large.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a zone set activation command that exceeds the size supported by the switch. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.						
Action:	Reduce the size of the zone set to conform to the limit specified, then retry the activation command.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 140							
Message:	Congestion detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeded the configured congestion threshold.						
Action:	No action is required for an isolated event. If this event persists, relieve the congestion by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte **0** = Port number reporting congestion.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 141							
Message:	Congestion relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that previously exceeded the configured congestion threshold. The congestion is now relieved.						
Action:	No action required.						
Event Data:	Byte **0** = Port number reporting congestion relieved.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 142							
Message:	Low BB_Credit detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This indicates downstream fabric congestion.						
Action:	No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If this event persists, relieve the low BB_Credit condition by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte **0** = Port number reporting low BB_Credit.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 143							
Message:	Low BB_Credit relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that previously exceeded the configured low BB_Credit threshold. The low-credit condition is now relieved.						
Action:	No action required.						
Event Data:	Byte **0** = Port number reporting low BB_Credit relieved.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 150							
Message:	Fabric merge failure.						
Severity:	Informational.						
Explanation:	During ISL initialization, the fabric merge process failed. The fabric binding membership lists do not match, an incompatible zone set was detected, there is a problem with exchanging zoning parameters, or the zone set merge failed. This event code is always preceded by a **070** ISL segmentation event code, and represents the reply of an adjacent fabric element. Refer to the event data for the failure reason.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	Event data are mapped from the software implementation of the FC-SW2 protocol and are typically complicated. Decoding the event data requires engineering support. Event data are as follows: Bytes **0 - 3** = Affected E_Port number(s). Bytes **4 - 7** = Request SW_ILS command codes. Bytes **8** - **31** = Request response payloads.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔				

<table>
<tr><th colspan="8">Event Code: 151</th></tr>
<tr><td>Message:</td><td colspan="7">Fabric configuration failure.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">A fabric-wide configuration activation process failed. An event code 151 is recorded only by the managing switch in the fabric. The event code is intended to help engineering support personnel fault isolate a fabric-wide configuration failures.</td></tr>
<tr><td>Action:</td><td colspan="7">Perform a data collection and return the CD to support personnel.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Event data are mapped from the software implementation of the FC-SW2 protocol and are typically complicated. Decoding the event data requires engineering support. Event data are as follows:

Bytes 0 - 3 = Managing switch domain ID in internal format (1-31).
Bytes 4 - 7 = Fabric configuration operation that failed.
Bytes 8 - 11 = Fabric configuration step that failed.
Bytes 12 - 15 = Managed switch domain ID in internal format (1-31).
Bytes 16 - 19 = Response command code received from the managed switch.
Bytes 20 - 23 = Response code received from the managed switch.
Bytes 24 - 27 = Reason code received from the managed switch.
Bytes 28 - 31 = Error code received from the managed switch.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Product</td><td colspan="3">Management Server</td><td colspan="2">Host</td></tr>
<tr><td>EFCM Basic Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident Log</td></tr>
<tr><td>✔</td><td>✔</td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Power Supply Events (200 through 299)

Event Code: 200							
Message:	Power supply AC voltage failure.						
Severity:	Major.						
Explanation:	AC input to the power supply is disconnected or AC circuitry in the power supply failed. The event only occurs when two power supplies are installed. The second power supply assumes the full operating load.						
Action:	Ensure the power supply is connected to facility AC power and verify operation of the facility power source. If the AC voltage does not recover (indicated by event code **203**), replace the failed power supply. Perform a data collection and return the CD and failed power supply to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 201							
Message:	Power supply DC voltage failure.						
Severity:	Major.						
Explanation:	DC circuitry in the power supply failed. The event only occurs when two power supplies are installed. The second power supply assumes the full operating load.						
Action:	Replace the failed power supply. Perform a data collection and return the CD and failed power supply to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 203							
Message:	Power supply AC voltage recovery.						
Severity:	Informational.						
Explanation:	AC voltage recovered for the power supply. Both power supplies adjust to share operating load.						
Action:	No action required.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 204							
Message:	Power supply DC voltage recovery.						
Severity:	Informational.						
Explanation:	DC voltage recovered for the power supply. Both power supplies adjust to share operating load.						
Action:	No action required.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 206							
Message:	Power supply removed.						
Severity:	Informational.						
Explanation:	A power supply was removed while the switch was powered on and operational. The second power supply assumes the full operating load.						
Action:	No action required or install an operational power supply.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 207							
Message:	Power supply installed.						
Severity:	Informational.						
Explanation:	A redundant power supply was installed with the switch powered on and operational. Both power supplies adjust to share operating load.						
Action:	No action required.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 208							
Message:	Power supply false shutdown.						
Severity:	Major.						
Explanation:	The power supply indicated that it was about to shutdown as a result of a power loss, but never did. The operational firmware prepared for the shutdown.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Fan Events (300 through 399)

Event Code: 300							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	One cooling fan failed or is rotating at insufficient angular velocity.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 301							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Two cooling fans failed or are rotating at insufficient angular velocity.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 302							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Three cooling fans failed or are rotating at insufficient angular velocity.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 303							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Fourth cooling fan failed or are rotating at insufficient angular velocity.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 304							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Fifth cooling fan failed or are rotating at insufficient angular velocity.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 305							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Sixth cooling fan failed or are rotating at insufficient angular velocity.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 310							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	One cooling fan recovered.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 311							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Two cooling fans recovered.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 312							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans recovered						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 313							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Four cooling fans recovered						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 314							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Five cooling fans recovered						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 315							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Six cooling fans recovered						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 370							
Message:	Cooling fan status polling temporarily disabled.						
Severity:	Minor.						
Explanation:	The failed or recovered status values for one or more cooling fans are exceeding a determined threshold. This indicates a possible fan failure. Fan status polling is enabled hourly or following an IML or reset.						
Action:	No immediate action required. Monitor cooling fan operation or additional event codes indicating a fan failure.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔		

CTP Card Events (400 through 499)

Event Code: 400							
Message:	Power-up diagnostics failure.						
Severity:	Major.						
Explanation:	Power-on self tests (POSTs) detected a failed FRU as indicated by the event data.						
Action:	If a CTP card or fan failure is indicated, replace the switch. If a power supply failure is indicated, replace the power supply. Perform a data collection and return the CD and faulty FRU to support personnel.						
Event Data:	Byte **0** = FRU code as follows: **02** = CTP card, **05** = cooling fan, **06** = power supply assembly. Byte **1** = FRU slot number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 410							
Message:	Switch reset.						
Severity:	Informational.						
Explanation:	The switch reset due to system power-up, IML, or manual reset. A software reset can occur automatically after a firmware fault (event code **411**), or be user-initiated. Event data indicates the type of reset.						
Action:	No action required.						
Event Data:	Byte **0** = reset type as follows: **00** = power-on, **02** = IML, **04** = reset.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 411							
Message:	Firmware fault.						
Severity:	Major.						
Explanation:	Switch firmware encountered an unexpected condition and dumped operating state information to FLASH memory for retrieval and analysis. The dump file automatically transfers to the management server, where it is stored for retrieval through a data collection. The switch performs a software reset, during which all attached Fibre Channel devices are momentarily disrupted, log out, and log back in.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	Bytes **0** - **3** = fault identifier, least significant byte first.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔			✔	

Event Code: 421							
Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A new firmware version was downloaded from the management server or EFCM Basic interface. Event data contains the ASCII firmware version in hexadecimal format **xx.yy.zz.bbbb**.						
Action:	No action required.						
Event Data:	Bytes **0** and **1** = release level (**xx**). Byte **2** = always a period. Bytes **3** and **4** = maintenance level (**yy**). Byte **5** = always a period. Bytes **6** and **7** = interim release level (**zz**). Byte **8** = always a space. Bytes **9** - **12** = build ID (**bbbb**).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 423							
Message:	CTP firmware download initiated.						
Severity:	Informational.						
Explanation:	The management server or EFCM Basic Edition interface initiated download of a new firmware version.						
Action:	No action required.						
Event Data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 433							
Message:	Nonrecoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A non-recoverable Ethernet interface failure was detected and the LAN connection to the management server or Internet was terminated. No failure information or event codes are reported outside the switch. Although Fibre Channel port functionality is not affected, the switch cannot be monitored or configured.						
Action:	Replace the switch.						
Event Data:	Byte **0** = LAN error type as follows: **01** = hard failure, **04** = registered fault. Byte **1** = LAN error subtype (internally defined). Byte **2** = LAN fault identifier (internally defined).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔				✔	

Event Code: 440							
Message:	Embedded port hardware failed.						
Severity:	Major.						
Explanation:	The embedded port hardware detected a fatal error.						
Action:	Replace the switch.						
Event Data:	Byte **0** = CTP slot position (**00**). Byte **1** = engineering reason code Bytes **4** - **7** = elapsed millisecond tick count.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 442							
Message:	Embedded port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the embedded port.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold or results in a port failure.						
Event Data:	Byte **0** = embedded port number. Byte **1** = anomaly reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** and **9** = HA error callout #1. Bytes **10** and **11** = HA error callout #2.			Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = HA error callout #3. Bytes **18** and **19** = HA error callout #4.			
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Port Events (500 through 599)

Event Code: 506							
Message:	Fibre Channel port failure.						
Severity:	Major.						
Explanation:	A Fibre channel port failed. The amber LED corresponding to the port illuminates to indicate the failure. Ports with LEDs extinguished remain operational.						
Action:	Perform a a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	Byte **0** = port number. Byte **1** = engineering reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = reason code specific. Byte **16** = connector type. Bytes **17** and **18** = transmitter technology. Byte **19** = distance capability. Byte **20** = supported transmission media. Byte **21** and **22** = speed capability.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 507							
Message:	Loopback diagnostics port failure.						
Severity:	Informational.						
Explanation:	A loopback diagnostic test detected a Fibre Channel port failure.						
Action:	No action required. An event code **506** is generated if this diagnostic failure results in a hard port failure.						
Event Data:	Byte **0** = port number. Byte **1** = engineering reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = reason code specific. Byte **12** = test type.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 508							
Message:	Fibre Channel port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the indicated Fibre Channel port.						
Action:	No action required. An event code **506** is generated if this anomaly results in a hard port failure.						
Event Data:	Byte **0** = port number. Byte **1** = anomaly reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** and **9** = HA error callout #1. Bytes **10** and **11** = HA error callout #2. Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = HA error callout #3. Bytes **18** and **19** = HA error callout #4.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 510							
Message:	Optical transceiver hot-insertion initiated.						
Severity:	Informational.						
Explanation:	Installation of an optical transceiver was initiated with the switch powered on and operational. The event indicates operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event Data:	Byte **0** = port number. Byte **2** = optic type. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 512							
Message:	Optical transceiver nonfatal error.						
Severity:	Minor.						
Explanation:	Switch firmware detected an optical transceiver non-fatal error.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte **0** = port number. Byte **1** = engineering reason code. Byte **2** = optic type. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 513							
Message:	Optical transceiver hot-removal completed.						
Severity:	Informational.						
Explanation:	An optical transceiver was removed while the switch was powered on and operational.						
Action:	No action required.						
Event Data:	Byte **0** = port number. Byte **2** = optic type. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 514							
Message:	Optical transceiver failure.						
Severity:	Major.						
Explanation:	An optical transceiver failed. The amber LED corresponding to the port illuminates to indicate the failure. Ports with LEDs extinguished remain operational.						
Action:	Replace the failed transceiver.						
Event Data:	Byte **0** = port number. Byte **1** = engineering reason code. Byte **2** = optic type. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 581							
Message:	Implicit incident.						
Severity:	Major.						
Explanation:	An attached server recognized a condition caused by an event that occurred at the server. The event caused an implicit Fibre Channel link incident.						
Action:	A link incident record (LIR) is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event Code: 582							
Message:	Bit error threshold exceeded.						
Severity:	Major.						
Explanation:	An attached server determined the number of code violation errors recognized exceeded the bit error threshold.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event Code: 583							
Message:	Loss of signal or loss of synchronization.						
Severity:	Major.						
Explanation:	An attached server recognized a loss-of-signal condition or a loss-of-synchronization condition that persisted for more than the specified receiver-transmitter timeout value (R_T_TOV).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event Code: 584							
Message:	Not operational primitive sequence received.						
Severity:	Major.						
Explanation:	An attached server received a not-operational primitive sequence (NOS).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event Code: 585							
Message:	Primitive sequence timeout.						
Severity:	Major.						
Explanation:	An attached server recognized either a link reset (LR) protocol timeout or a timeout while waiting for the appropriate response (while in a NOS receive state and after NOS was not longer recognized).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event Code: 586							
Message:	Invalid primitive sequence received for current link state.						
Severity:	Major.						
Explanation:	An attached server recognized either a link reset (LR) or a link-reset response (LRR) sequence while in the wait-for-online sequence (OLS) state.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event Code: 604							
Message:	EOS: SBAR module failure. EOSN: SWM module failure						
Severity:	Major.						
Explanation:	A failure criterion associated with the SWM/serial crossbar hardware module has been met.						
Action:	Perform a data collection and return the CD to support personnel.						
Event Data:	Byte **0** =port number Byte **1**= BMAC link number						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

B

Restore Management Server

This appendix describes the procedure to restore a rack-mount management server after a hard drive failure. The procedure includes restoration of the:

- Windows operating system.
- Windows configuration information.
- Storage area network (SAN) management and Element Manager applications.
- SAN management data directory.

Requirements

The following are required:

- ***Management Server Restore* CD-ROM -** This CD-ROM is shipped with the management server and contains the:
  - — Disk operating system (DOS) files required to boot the server after a hard drive failure.
  - — Windows operating system.
- ***EFC Management Applications* CD-ROM -** This CD-ROM contains the SAN management and product Element Manager applications.

- **SAN Management data directory backup on CD-ROM -** The SAN management data directory is automatically backed up to a CD when the server is rebooted or when the data directory contents change. The data directory includes:
  - — Configuration data (product definitions, user names, passwords, user rights, nicknames, session options, simple network management protocol (SNMP) trap recipients, E-mail recipients, and Ethernet event notifications).
  - — Log files (SAN management application logs and individual Element Manager logs).
  - — Zoning library (all zone set and zone definitions).
  - — Firmware library.
  - — Call-home settings.
  - — Configuration data for each managed product (stored on the server and in NV-RAM on each product).
- **Windows configuration information -** Windows operating system network addresses, date and time information, user information, and product identification are recorded during installation of the server. Refer to *Task 14: Record or Verify Server Restore Information* for information.

Restore Management Server Procedure

To restore the server:

1. At the server, press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive.
2. Insert the ***Management Server Restore*** CD-ROM in the CD-RW drive and close the LCD panel.

ATTENTION ! This procedure deletes all data from the C: hard drive partition.

---

3. Press the power (⏻) button. The server powers on and performs the restore process from the CD-ROM.
4. After the restore process completes, the server makes an audible series of beeps. Remove the ***Management Server Restore*** CD-ROM from the CD-RW drive.

5. Power cycle the server. The server performs power-on self-tests (POSTs). After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
6. Configure the following parameters at the server's LCD panel. Refer to *Task 7: Configure Server Password and Network Addresses* for instructions.
   - LCD panel password.
   - IP address for private and public LAN connections.
   - Subnet mask or private and public LAN connections.
7. Log on to the server's Windows desktop through a LAN connection to a browser-capable PC. Refer to *Access the Management Server Desktop* for instructions.
8. Configure Windows operating system information as required by the customer:
   - Configure computer and workgroup names for the server. If required, change the server's gateway address and DNS server IP address to conform to the customer's LAN addressing scheme. Refer to *Task 8: Configure Management Server Information* for instructions.
   - Change the default Windows administrator password and configure password access for users. Refer to *Task 9: Configure Windows Operating System Users* for instructions.
   - Set the server's date and time. Refer to *Task 10: Set Management Server Date and Time* for instructions.
   - Configure the call-home feature. Refer to *Task 11: Configure the Call-Home Feature (Optional)* for instructions.
9. Insert the ***EFC Management Applications*** CD-ROM in the CD-RW drive and close the LCD panel.
10. At the server's Windows desktop, click *Start* at the left side of the task bar, then select the *Run* option. The *Run* dialog box displays.
11. At the *Run* dialog box, type **`D:\mcdataServerInstall.exe`** in the *Open* field.
12. Click *OK*. The *InstallShield* third-party application prepares to install the software version, and opens the *InstallShield Wizard* dialog box (Figure B-1).

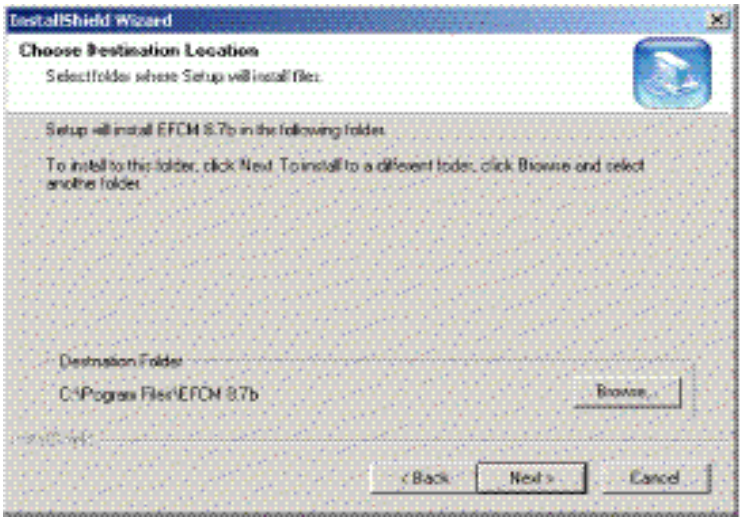

InstallShield Wizard
Choose Destination Location
Select folder where Setup will install files.
Setup will install EFCM 8.7b in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\EFCM 8.7b
Browse...
InstallShield
< Back
Next >
Cancel

Figure B-1 InstallShield Wizard Dialog Box

13. Remove the ***EFC Management Applications*** CD-ROM from the CD-RW drive.
14. Insert the SAN management data directory backup CD-ROM (created while performing *Task 20: Back Up Configuration Data*) in the CD-RW drive and close the LCD panel.
15. Copy the contents of the CD-ROM to the server hard drive as follows:
    - For the EFCM 8.7 application, copy the CD-ROM contents to the following directories:
      - **C:\Program Files\EFCM 8.7\CallHome**
      - **C:\Program Files\EFCM 8.7\Client**
      - **C:\Program Files\EFCM 8.7\Server**.
16. Power off and reboot the server.
    a. At the Windows desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays.

b. Select the *Restart* option from the list box and click *OK*. The server powers down and restarts. During the reboot process the LAN connection between the server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error.

c. After the server reboots, click *Login again*. The *VNC Authentication* screen displays.

d. Type the default password and click *OK*. The *Welcome to Windows* dialog box displays.

NOTE: The default TightVNC viewer password is **password.**

---

e. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the server desktop. The *Log On to Windows* dialog box displays.

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the rack-mount management server.

---

f. Type the default Windows user name and password and click *OK*. The server's Windows desktop opens and the *EFCM Log In* dialog box displays.

NOTE: The default Windows user name is **Administrator** and the default password is **password**. Both are case-sensitive.

---

g. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default SAN management application user ID is **Administrator** and the default password is **password.** Both are case-sensitive.

---

h. Click *Login*. The application opens and the main window appears.

Index

A

access control list
  configure
    Element Manager 2-73
  description 2-73
attention statements xxiv
authentication
  access control list 2-73
  configure
    EFCM Basic 2-29
    Element Manager 2-73
    SAN management application 2-73
  RADIUS server support 2-30, 2-73
  settings 2-29, 2-73
authentication settings
  configure
    EFCM Basic 2-29
    Element Manager 2-73
  description 2-29, 2-73

B

back up
  SAN management application configuration data 2-75
  switch configuration file
    EFCM Basic Edition 4-25
    Element Manager 4-51
BB_Credit
  configure
    EFCM Basic 2-22
    Element Manager 2-65
  description 2-22, 2-65
binding
  fabric
    configure through EFCM Basic 2-30
    configure through SAN management application 2-73
    enable through EFCM Basic 2-30
    enable through SAN management application 2-73
    Enterprise Fabric Mode 2-30, 2-73
  port
    configure through EFCM Basic 2-30
    configure through Element Manager 2-66
    enable through EFCM Basic 2-30
    enable through Element Manager 2-66
  switch
    configure through EFCM Basic 2-30
    configure through Element Manager 2-74
    enable through EFCM Basic 2-30
    enable through Element Manager 2-74
block port
  EFCM Basic Edition 4-22
  Element Manager 4-47

C

call-home support
  configure at management server 2-48, 2-72
  enable at management server 2-72
chassis ground connector
  description 1-6
  location 1-3
clean fiber-optic components 4-5
clearances 1-7

command line interface
disable 2-24
enable 2-24
compliance statements
Argentinian UL Certification xxi
Australia C-Tick Mark xxi
Canadian EMC xix
CB Scheme xx
Chinese BSMI Statement xxii
Chinese CCC Mark xxii
Class 1 laser transceiver xviii
European Union CE Mark xx
European Union N-Mark xxi
Federal Communications Commission xviii
German GS Mark xxii
Japanese VCCI Statement xxii
Korean MIC Mark xxiii
Mexican NOM Mark xxiii
New Zealand C-Tick Mark xxi
recycling information xxiii
Russian GOST Certification xxiii
South African SABS Certification xxiii
UL Certification xx
configuration file
back up
EFCM Basic Edition 4-25
Element Manager 4-51
restore
EFCM Basic Edition 4-26
Element Manager 4-51
configure
access control list
Element Manager 2-73
authentication settings
EFCM Basic 2-29
Element Manager 2-73
basic port information
EFCM Basic 2-21
Element Manager 2-64
call-home feature 2-48
call-home support 2-72
Element Manager application 2-59
e-mail notification 2-70
Enterprise Fabric Mode
EFCM Basic 2-30
SAN management application 2-73
Ethernet events 2-72
fabric binding
EFCM Basic 2-30
SAN management application 2-73
fabric parameters
EFCM Basic 2-17
Element Manager 2-62
ISL performance features
EFCM Basic 2-30
Element Manager 2-74
SAN management application 2-74
management server
date and time 2-46
DNS domain name 2-40
IP address 2-38
name 2-40
password 2-38
subnet mask 2-38
OpenTrunking
EFCM Basic 2-30
Element Manager 2-74
OSMS
EFCM Basic 2-25
Element Manager 2-56
passwords 2-38, 2-49
PFE keys
EFCM Basic 2-27
Element Manager 2-55
port BB_Credit
EFCM Basic 2-22
Element Manager 2-65
port binding
EFCM Basic 2-30
Element Manager 2-66
port fencing
EFCM Basic 2-31
SAN management application 2-74
port NPIV
EFCM Basic 2-22
Element Manager 2-66
preferred path
EFCM Basic 2-30
Element Manager 2-74
RADIUS server
EFCM Basic 2-30
Element Manager 2-73
SANtegrity authentication
EFCM Basic 2-29

Element Manager 2-73
SANtegrity binding
EFCM Basic 2-29
Element Manager 2-73
SAN management application 2-73
security features
EFCM Basic 2-29
Element Manager 2-73
SAN management application 2-73
SNMP
EFCM Basic 2-23
Element Manager 2-66
SSL encryption
software 2-25
web 2-25
switch binding
EFCM Basic 2-30
Element Manager 2-74
switch date and time
EFCM Basic 2-15
Element Manager 2-57
switch identification
EFCM Basic 2-14
Element Manager 2-59
switch network information
EFCM Basic 2-19
maintenance port 2-32
switch operating parameters
EFCM Basic 2-16
Element Manager 2-61
switch to SAN management application 2-51
threshold alerts 2-68
user names 2-49
Windows users 2-44
zone sets 2-78
zones 2-78
cooling fan
description 1-4
events (300 - 399) A-28
fault isolation 3-24
illustrated parts breakdown 6-3
CTP card
events (400 - 499) A-35
fault isolation 3-24
firmware versions 4-23, 4-48

D

danger statements xxiv
data collection procedure
EFCM Basic Edition 4-20
Element Manager 4-45
date
set at management server 2-46
set switch date
EFCM Basic 2-15
Element Manager 2-57
default
DNS server IP address 2-52
EFCM Basic Edition
password 2-12
user name 2-12
maintenance port password 2-34, 3-22
management server
gateway address 2-52
IP address 2-52
LCD panel password 2-38
subnet mask 2-52
SAN management application
password 2-49, 2-77, 4-57, B-5
user name 2-49, 2-77, 4-57, B-5
switch
gateway address 2-1, 3-1
IP address 2-1, 3-1
passwords 2-1, 3-1
subnet mask 2-1, 3-1
TightVNC password 2-41, 2-76, 4-57, B-5
Windows
password 2-41, 2-77, 4-57, B-5
user name 2-41, 2-77, 4-57, B-5
dimensions 1-7
door key
description 1-14
illustration 1-14
download
firmware
EFCM Basic Edition 4-24
Element Manager 4-49
from filecenter 4-6
software from filecenter 4-6

E

E_D_TOV 2-18

E_Port
configure 2-21, 2-64
description 1-2
OpenTrunking 2-30, 2-74
performance features 2-30, 2-74
port fencing 2-31, 2-74
preferred path 2-30, 2-74
segmented 3-41
e_port segmentation
reasons for 4-38
EFCM Basic Edition
configure product 2-12
disable at management server 2-70
embedded port frame log 4-12
enable at management server 2-70
event log 4-10
fabric log 4-12
link incident log 4-11
open trunking re-route log 4-12
Element Manager application
configure 2-59
configure PFE key
EFCM Basic 2-27
Element Manager 2-55
embedded port log 4-33
event log 4-31
hardware log 4-31
link incident log 4-31
open trunking log 4-33
port threshold alert log 4-32
switch fabric log 4-34
e-mail support
configure at management server 2-70
enable at management server 2-70
embedded port frame log 4-12
embedded port log 4-33
enable
call-home support 2-72
command line interface 2-24
EFCM Basic Edition 2-70
e-mail notification 2-70
Enterprise Fabric Mode
EFCM Basic 2-30
SAN management application 2-73
Ethernet events 2-72
host control
EFCM Basic 2-25
Element Manager 2-56
port binding
EFCM Basic 2-30
Element Manager 2-66
SSL encryption
software 2-25
web 2-25
switch binding
EFCM Basic 2-30
Element Manager 2-74
Telnet access 2-70
Enterprise Fabric Mode
configure
EFCM Basic 2-30
SAN management application 2-73
description 2-30, 2-73
enable
EFCM Basic 2-30
SAN management application 2-73
environment
operating 1-8
shipping 1-7
storage 1-7
ERR LED
description 1-6
location 1-3
error detection
description 1-12
event codes 3-2
error reporting
description 1-12
event codes 3-2
ESD
precautions xxv
RRP precautions 5-2
Ethernet connector
description 1-5
location 1-3
Ethernet events
configure at management server 2-72
enable at management server 2-72
Ethernet hub
description 1-11
fault isolation 3-14
illustration 1-12
installation 2-5
event codes

cooling fan events (300 - 399) A-28
CTP card events (400 - 499) A-35
description A-1
port events (500 - 599) A-39
power supply events (200 - 299) A-24
system events (000 - 199) A-2
event log
EFCM Basic Edition 4-10
Element Manager 4-31
SAN management 4-29
external loopback test
description 4-19, 4-42
EFCM Basic Edition 4-19
Element Manager 4-42

F

F_Port
configure 2-21, 2-64
description 1-1
fabric binding
configure
EFCM Basic 2-30
SAN management application 2-73
description 2-30, 2-73
enable
EFCM Basic 2-30
SAN management application 2-73
Enterprise Fabric Mode 2-30, 2-73
fabric log
EFCM Basic Edition 4-12
SAN management 4-29
fabric parameters (configure)
EFCM Basic 2-17
Element Manager 2-62
Fabricenter equipment cabinet
description 1-2
Ethernet hub installation 2-7
management server installation 2-36
switch installation 2-11
fault isolation
MAP 0000 - Start MAP 3-5
MAP 0100 - Power distribution analysis 3-10
MAP 0200 - POST failure analysis 3-13
MAP 0300 - Loss of server communication 3-14
MAP 0400 - FRU failure analysis 3-24
MAP 0500 - Port failure or link incident analysis 3-26
MAP 0600 - Fabric or ISL problem analysis 3-38
summary 3-2
fenced E_Port
description 3-46
fault isolation 3-38
fiber-optic protective plug
description 1-15
illustration 1-15
filecenter
download firmware 4-6
download software 4-6
registration 2-80
firmware
add version to management server library 4-49
determine version
EFCM Basic Edition 4-23
Element Manager 4-48
download
EFCM Basic Edition 4-24
Element Manager 4-49
version from filecenter 4-6
FL_Port
configure 2-21, 2-64
description 1-2
Flexport Technology
configure PFE key
EFCM Basic 2-27
Element Manager 2-55
description 2-27, 2-55
FRU removal
power supply 5-7
SFP transceiver 5-3
tools required 5-3, 5-7
FRU replacement
power supply 5-8
SFP transceiver 5-5
tools required 5-3, 5-7
FRUs
description 1-2
illustrated parts breakdown 6-1
power supply 1-4
SFP transceiver 1-3
status LEDs 1-6

full-volatility feature
configure PFE key
EFCM Basic 2-27
Element Manager 2-55
description 4-20, 4-45

G

gateway address
change switch address 2-19, 2-32
management server default 2-52
switch default 2-1, 3-1

H

hardware log 4-31

I

identification (configure)
EFCM Basic 2-14
Element Manager 2-59
illustrated parts breakdown
front-accessible FRUs 6-2
miscellaneous parts 6-4
power cords 6-5
rear-accessible FRUs 6-3
IML switch 4-4
installation tasks
summary 2-2
Task 1 - Verify installation requirements 2-4
Task 10 - Set management server date and time 2-46
Task 11 - Configure the call-home feature (optional) 2-48
Task 12 - Assign user names and passwords 2-49
Task 13 - Configure the product to the management application 2-51
Task 14 - Record or verify server restore information 2-52
Task 15 - Verify product-to-server communication 2-53
Task 16 - Configure PFE key (optional) 2-55
Task 17 - Configure management server (optional) 2-56
Task 18 - Set product date and time 2-57
Task 19 - Configure the Element Manager application 2-59
Task 2 - Unpack, inspect, and install the Ethernet hub (optional) 2-5
Task 20 - Back up configuration data 2-75
Task 21 - Cable Fibre Channel ports 2-77
Task 22 - Configure zoning (optional) 2-78
Task 23 - Connect product to a fabric element (optional) 2-79
Task 24 - Register with the McDATA filecenter 2-80
Task 3 - Unpack, inspect, and install the product 2-9
Task 4 - Configure product at the EFCM Basic Edition interface (optional) 2-12
Task 5 - Configure product network information (optional) 2-32
Task 6 - Unpack, inspect, and install the management server 2-35
Task 7 - Configure server password and network addresses 2-38
Task 8 - Configure management server information 2-40
Task 9 - Configure Windows operating system users 2-44
internal loopback test
description 4-17, 4-41
EFCM Basic Edition 4-17
Element Manager 4-41
interop mode 2-18, 2-64
interswitch link
configure performance features
EFCM Basic 2-30
Element Manager 2-74
SAN management application 2-74
description 1-2
fault isolation 3-38
OpenTrunking 2-30, 2-74
port fencing 2-31, 2-74
preferred path 2-30, 2-74
IP address
change switch address 2-19, 2-32
DNS server default 2-52
management server default 2-52
switch default 2-1, 3-1

L

LAN connection
  connect management server 2-35
laser transceiver
  compliance statement xviii
  description 1-3
  illustrated parts breakdown 6-2
  removal 5-3
  replacement 5-5
  types available 1-3
LCD panel
  configure private server network addresses 2-39
  configure public server network addresses 2-39
  default password for management server 2-38
LEDs
  ERR 1-6
  port status 1-6
  power supply status 1-6
  PWR 1-6
link incident log
  EFCM Basic Edition 4-11
  Element Manager 4-31
logs
  embedded port 4-33
  embedded port frame 4-12
  event
    EFCM Basic 4-10
    Element Manager 4-31
    SAN management 4-29
  fabric
    EFCM Basic 4-12
    SAN management 4-29
  hardware 4-31
  link incident
    EFCM Basic 4-11
    Element Manager 4-31
  open trunking 4-33
  open trunking re-route
    EFCM Basic 4-12
  port threshold alert 4-32
  product status 4-29
  switch fabric 4-34
loopback plug
  description 1-14
  illustration 1-14
loopback test
  external
    EFCM Basic Edition 4-19
    Element Manager 4-42
  internal
    EFCM Basic Edition 4-17
    Element Manager 4-41

M

MAC address, switch 2-32
maintenance analysis procedures
  MAP 0000 - Start MAP 3-5
  MAP 0100 - Power distribution analysis 3-10
  MAP 0200 - POST failure analysis 3-13
  MAP 0300 - Loss of server communication 3-14
  MAP 0400 - FRU failure analysis 3-24
  MAP 0500 - Port failure or link incident analysis 3-26
  MAP 0600 - Fabric or ISL problem analysis 3-38
  summary 3-2
maintenance approach 1-8
maintenance port
  configure switch network addresses 2-32
  default password 2-34, 3-22
  description 1-6
  location 1-3
manage configuration data
  EFCM Basic Edition 4-25
  Element Manager 4-51
management server
  access through TightVNC 2-40
  description 1-9
  event code tables A-1
  fault isolation 3-14
  illustration 1-10
  installation 2-35
  LCD panel password 2-38
  minimum specifications 1-10
  recommended specifications 1-11
  restore procedure B-2
  restore requirements B-1
  specifications 1-10

multiswitch fabric
e_port segmentation
reasons for 4-38

N

N_Port ID virtualization
configure PFE key
EFCM Basic 2-27
Element Manager 2-56
description 2-22, 2-66
network information
configure management server 2-38
configure switch
EFCM Basic 2-19
maintenance port 2-32
NPIV
configure
EFCM Basic 2-22
Element Manager 2-66
description 2-22, 2-66
null modem cable
description 1-15
illustration 1-15

O

open trunking log 4-33
open trunking re-route log 4-12
open-systems management server (configure)
EFCM Basic 2-25
Element Manager 2-56
OpenTrunking
configure
EFCM Basic 2-30
Element Manager 2-74
configure PFE key
EFCM Basic 2-27
Element Manager 2-56
description 2-30, 2-74
operating environment 1-8
operating parameters (configure)
EFCM Basic 2-16
Element Manager 2-61

P

password
configure at management server 2-49
customer-level switch 2-1, 3-1
default
management server LCD panel 2-38
default EFCM Basic Edition 2-12
default maintenance port 2-34, 3-22
default SAN management application 2-49, 2-77, 4-57, B-5
default server 2-38
default TightVNC 2-41, 2-76, 4-57, B-5
default Windows 2-41, 2-77, 4-57, B-5
maintenance-level switch 2-1, 3-1
performance statistics
Class 2
EFCM Basic Edition 4-17
Class 3
EFCM Basic Edition 4-17
error
EFCM Basic Edition 4-17
open trunking 4-17
traffic
EFCM Basic Edition 4-17
PFE keys
configure
EFCM Basic 2-27
Element Manager 2-55
Element Manager application 2-27, 2-55
Flexport Technology 2-27, 2-55
full-volatility 2-27, 2-55
N_Port ID virtualization 2-27, 2-56
OpenTrunking 2-27, 2-56
SANtegrity (enhanced) 2-27, 2-56
port binding
configure
EFCM Basic 2-30
Element Manager 2-66
description 2-30, 2-66
enable
EFCM Basic 2-30
Element Manager 2-66
port fencing
configure
EFCM Basic 2-31
SAN management application 2-74
description 2-31, 2-74
port threshold alert log 4-32
ports

cabling 2-77
configurable types 1-1
configure basic information
EFCM Basic 2-21
Element Manager 2-64
configure BB_Credit
EFCM Basic 2-22
Element Manager 2-65
configure NPIV
EFCM Basic 2-22
Element Manager 2-66
E_Port fencing 2-31, 2-74
events (500 - 599) A-39
LED diagnostics 4-8
performance statistics
EFCM Basic Edition 4-17
Element Manager 4-36
port properties 4-37
port technology 4-39
SFP transceivers 1-3
status LEDs 1-6
swap ports 4-44
power cords
description 6-5
illustrated parts breakdown 6-5
power requirements 1-7
power supply
connector location 1-3
description 1-4
events (200 - 299) A-24
fault isolation 3-10
illustrated parts breakdown 6-3
removal 5-7
replacement 5-8
status LED 1-6
power-off procedure 4-3
power-on procedure 4-2
precautions
ESD xxv
general xxv
preferred domain ID 2-61
preferred path
configure
EFCM Basic 2-30
Element Manager 2-74
description 2-30, 2-74
procedural notes 4-2
procedures
EFCM Basic Edition
block or unblock port 4-22
data collection 4-20
manage configuration data 4-25
obtain log information 4-10
set online state 4-21
upgrade firmware 4-23
Element Manager
block or unblock port 4-47
data collection 4-45
manage configuration data 4-51
obtain switch log information 4-30
perform port diagnostics 4-35
set online state 4-46
swap ports 4-44
upgrade firmware 4-48
installation 2-2
power-off 4-3
power-on 4-2
repair 4-1
SAN management application
install or upgrade software 4-55
obtain fabric log information 4-29
product status log 4-29
publications, related xvi
PWR LED
description 1-6
location 1-3

R

R_A_TOV 2-18
rack-mount installation
Ethernet hub 2-7
management server 2-36
switch 2-11
RADIUS server
configure
EFCM Basic 2-30
Element Manager 2-73
description 2-30, 2-73
recycling information xxiii
remove and replace procedures
ESD precautions 5-2
FRU list 5-2
procedural notes 5-1

repair procedures
clean fiber-optic components 4-5
download firmware or software 4-6
EFCM Basic Edition
block or unblock port 4-22
collect maintenance data 4-20
manage configuration data 4-25
obtain log information 4-10
set online state 4-21
upgrade firmware 4-23
Element Manager
block or unblock port 4-47
collect maintenance data 4-45
manage configuration data 4-51
obtain switch log information 4-30
perform port diagnostics 4-35
set online state 4-46
swap ports 4-44
upgrade firmware 4-48
IML or reset switch 4-3
overview 4-1
port LED diagnostics 4-8
power-off procedure 4-3
power-on procedure 4-2
SAN management application
install or upgrade software 4-55
obtain fabric log information 4-29
rerouting delay 2-62
reset
configuration data
EFCM Basic Edition 4-27
Element Manager 4-52
switch 4-4
RESET button
function 1-5
location 1-3
restore
management server B-2
switch configuration file
EFCM Basic Edition 4-26
Element Manager 4-51

S

safety
attention statements xxiv
danger statements xxiv
ESD precautions xxv, 5-2
general precautions xxv
SAN management application
default
password 2-49, 2-77, 4-57, B-5
user name 2-49, 2-77, 4-57, B-5
event log 4-29
fabric log 4-29
product status log 4-29
SANtegrity (enhanced)
configure PFE key
EFCM Basic 2-27
Element Manager 2-56
SANtegrity authentication
access control list 2-73
configure
EFCM Basic 2-29
Element Manager 2-73
RADIUS server support 2-30, 2-73
settings 2-29, 2-73
SANtegrity binding
configure
EFCM Basic 2-29
Element Manager 2-73
SAN management application 2-73
Enterprise Fabric Mode
configure through EFCM basic 2-30
configure through SAN management application 2-73
fabric binding
configure through EFCM basic 2-30
configure through SAN management application 2-73
port binding
configure through EFCM basic 2-30
configure through Element Manager 2-66
switch binding
configure through EFCM basic 2-30
configure through Element Manager 2-74
security features
configure
EFCM Basic 2-29
Element Manager 2-73
SAN management application 2-73
Enterprise Fabric Mode 2-29, 2-73

SANtegrity authentication 2-29, 2-73
SANtegrity binding 2-29, 2-73
segmented E_Port
description 3-41
fault isolation 3-38
serviceability features 1-12
set online state
EFCM Basic Edition 4-21
Element Manager 4-46
SFP transceiver
description 1-3
fault isolation 3-26
illustrated parts breakdown 6-2
removal 5-3
replacement 5-5
types available 1-3
shipping environment 1-7
SNMP
configure
EFCM Basic 2-23
Element Manager 2-66
description 2-23, 2-66
software
download version from filecenter 4-6
install 4-55
upgrade 4-55
specifications
management server 1-10
switch clearances 1-7
switch dimensions 1-7
switch power requirements 1-7
Sphereon 4400 Fabric Switch
description 1-1
FRU removal and replacement 5-1
FRUs 1-2
illustrated parts breakdown 6-1
installation 2-9
maintenance approach 1-8
management 1-9
repair procedures 4-1
specifications 1-6
SSL encryption
configure software encryption 2-25
configure web encryption 2-25
storage environment 1-7
subnet mask
change switch value 2-19, 2-32
management server default 2-52
switch default 2-1, 3-1
swap ports 4-44
switch binding
configure
EFCM Basic 2-30
Element Manager 2-74
description 2-30, 2-74
enable
EFCM Basic 2-30
Element Manager 2-74
switch fabric log 4-34
switch priority 2-18, 2-63
system events (000 - 199) A-2

T

technical support
filecenter registration 2-80
technical support center
e-mail address xvii
fax number xvii
phone number xvii
technical support center
e-mail address xvii
fax number xvii
phone number xvii
Telnet access
disable at management server 2-70
enable at management server 2-70
test
call-home support 2-72
e-mail notification 2-70
threshold alert
port properties dialog box 4-38
reasons for 4-38
threshold alerts
configure 2-68
description 2-68
types 2-68
TightVNC
access management server 2-40
default password 2-41, 2-76, 4-57, B-5
time
set at management server 2-46
set switch time
EFCM Basic 2-15

Element Manager 2-57
tools and test equipment
FRU removal and replacement 5-3, 5-7
supplied by service personnel 1-15
supplied with product 1-14
trademarks xviii

U

unblock port
EFCM Basic Edition 4-22
Element Managerapplication 4-47
user name
configure at management server 2-49
default EFCM Basic Edition 2-12
default SAN management application 2-49, 2-77, 4-57, B-5
default Windows 2-41, 2-77, 4-57, B-5

V

verify
management server restore information 2-52
power supply replacement 5-9
SFP transceiver replacement 5-5
switch-to-server communication 2-53

W

Windows
configure users 2-44
default
password 2-41, 2-77, 4-57, B-5
user name 2-41, 2-77, 4-57, B-5
WWN
port properties dialog box 4-37

Z

zone sets
configure
EFCM Basic 2-78
Element Manager 2-78
description 2-78
naming conventions 2-78
zones
configure
EFCM Basic 2-78
Element Manager 2-78
description 2-78
naming conventions 2-78